# NAVAL POSTGRADUATE SCHOOL

**MONTEREY, CALIFORNIA**

# THESIS

**SUPPORTING COMMAND AND CONTROL (C2) OF AN EMBARKED COMMANDER: TUNNELING SIPRNET DATA ACROSS AN UNCLAS WIRELESS LAN**

by

Erik R. Marshburn

September 2011

| | |
|---|---|
| Thesis Advisor: | Douglas MacKinnon |
| Co-Advisor: | John H. Gibson |

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

| REPORT DOCUMENTATION PAGE | | | *Form Approved OMB No. 0704–0188* |
|---|---|---|---|



| **1. AGENCY USE ONLY *(Leave blank)*** | **2. REPORT DATE** September 2011 | **3. REPORT TYPE AND DATES COVERED** Master's Thesis |
|---|---|---|

| | |
|---|---|
| **4. TITLE AND SUBTITLE** Supporting Command and Control (C2) of an Embarked Commander: Tunneling SIPRNet Data across an UNCLAS Wireless LAN | **5. FUNDING NUMBERS** |
| **6. AUTHOR(S)** Erik R. Marshburn | |
| **7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)** Naval Postgraduate School Monterey, CA 93943–5000 | **8. PERFORMING ORGANIZATION REPORT NUMBER** |
| **9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)** N/A | **10. SPONSORING/MONITORING AGENCY REPORT NUMBER** |

**11. SUPPLEMENTARY NOTES** The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ___N/A______.

| **12a. DISTRIBUTION / AVAILABILITY STATEMENT** Approved for public release; distribution is unlimited | **12b. DISTRIBUTION CODE** |
|---|---|

**13. ABSTRACT (maximum 200 words)**

Command and Control (C2) by today's embarked commanders requires timely and reliable access to classified data systems at the C2 node provided by the ship. Most often, the ship's spaces provided to an embarked staff are inadequate to support the commander's C2 requirements. Often, there are not enough classified computers or classified Local Area Network (LAN) connections. To facilitate improved ability to exercise C2, a ship's company technicians typically place a hub on the network to provide extra connection points. This procedure takes time for the technicians to implement and requires physical connection to the wired network. A potential alternative may be to leverage current IEEE 802.11 technology to provide wireless connectivity for these clients, yet wireless technology alone will not address this problem. Coupling an 802.11 network with Secret Client Tunneling Device (SCTD)-enabled classified laptops can provide the access to classified data that is required by the embarked commander to exercise command and control of his assigned forces. This thesis examines the use of the KOV-26 Talon card and the KIV-54 cryptographic module, both NSA Type I encryptors, as a method of tunneling SIPRNet data across an afloat unclassified wireless Local Area Network (LAN).

| | |
|---|---|
| **14. SUBJECT TERMS** Command and Control (C2), Wireless Local Area Network (WLAN), 802.11, Data Tunneling | **15. NUMBER OF PAGES** 91 |
| | **16. PRICE CODE** |

| **17. SECURITY CLASSIFICATION OF REPORT** | **18. SECURITY CLASSIFICATION OF THIS PAGE** | **19. SECURITY CLASSIFICATION OF ABSTRACT** | **20. LIMITATION OF ABSTRACT** |
|---|---|---|---|
| Unclassified | Unclassified | Unclassified | UU |

NSN 7540–01–280–5500

Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**SUPPORTING COMMAND AND CONTROL (C2) OF AN EMBARKED COMMANDER: TUNNELING SIPRNET DATA ACROSS AN UNCLAS WIRELESS LAN**


Erik R. Marshburn
Commander, United States Navy
B.S., University of Kansas, 1993


Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION TECHNOLOGY MANAGEMENT**

from the

**NAVAL POSTGRADUATE SCHOOL**
**September 2011**

Author: Erik R. Marshburn

Approved by: Douglas J. MacKinnon
Thesis Advisor

John H. Gibson
Thesis Co-Advisor

Dan Boger
Chair, Department of Information Sciences

THIS PAGE INTENTIONALLY LEFT BLANK

# ABSTRACT

Command and Control (C2) by today's embarked commanders requires timely and reliable access to classified data systems at the C2 node provided by the ship. Most often, the ship's spaces provided to an embarked staff are inadequate to support the commander's C2 requirements. Often, there are not enough classified computers or classified Local Area Network (LAN) connections. To facilitate improved ability to exercise C2, a ship's company technicians typically place a hub on the network to provide extra connection points. This procedure takes time for the technicians to implement and requires physical connection to the wired network. A potential alternative may be to leverage current IEEE 802.11 technology to provide wireless connectivity for these clients, yet wireless technology alone will not address this problem. Coupling an 802.11 network with Secret Client Tunneling Device (SCTD)-enabled classified laptops can provide the access to classified data that is required by the embarked commander to exercise command and control of his assigned forces. This thesis examines the use of the KOV-26 Talon card and the KIV-54 cryptographic module, both NSA Type I encryptors, as a method of tunneling SIPRNet data across an afloat unclassified wireless Local Area Network (LAN).

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

# LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

# LIST OF ACRONYMS AND ABBREVIATIONS

| | |
|---|---|
| AES | Advanced Encryption System |
| AO | Area of Operations |
| C2 | Command and Control |
| C4I | Command, Control, Communications, Computers, and Intelligence |
| CANES | Consolidated Afloat Networks and Enterprise Services |
| CaS | Collaboration at Sea |
| CCI | Controlled Cryptographic Item |
| CENTRIXS | Coalition Enterprise Regional Information Exchange System |
| CIC | Combat Information Center |
| COTS | Commercial Off-the-Shelf |
| DESRON | Destroyer Squadron |
| DoD | Department of Defense |
| DSSS | Direct Sequence Spread Spectrum |
| EAP-TLS | Extensible Authentication Protocol-Transport Layer Security |
| EMOD | Ethernet Module |
| FHSS | Frequency Hopping Spread Spectrum |
| FIPS | Federal Information Processing Standards |
| GOTS | Government Off-the-Shelf |
| HAIPE | High Assurance Internet Protocol Encryption |
| HR-DSSS | High Rate-Direct Sequence Spread Spectrum |
| IA | Information Assurance |
| IEEE | Institute of Electrical and Electronics Engineers |
| IR | Infra-red |
| ISM | Industrial, Scientific, and Medical |
| LAN | Local Area Network |
| Mbps | Megabits per second |
| NIPRNet | Non-secret Internet Protocol Router Network |
| NSA | National Security Agency |
| OFDM | Orthogonal Frequency Division Multiplexing |
| OSI | Open Systems Interconnection |
| PCMCIA | Personal Computer Memory Card International Association |

| | |
|---|---|
| PoE | Power over Ethernet |
| RMOD | Radio Module |
| SCTD | Secret Client Tunneling Device |
| SIPRNet | Secret Internet Protocol Router Network |
| SME | Subject Matter Expert |
| SSL | Secure Socket Layer |
| SSO | Site Security Officer |
| STAO | Staff Tactical Action Officer |
| TACTAS | Tactical Towed Array Sonar |
| THS | Talon Host Software |
| TLS | Transport Layer Security |
| TS/SCI | Top Secret/Sensitive Compartmented Information |
| TW | Trident Warrior |
| WLAN | Wireless Local Area Network |

# ACKNOWLEDGMENTS

I would like to first thank my beautiful wife and our three wonderful daughters. Without your tremendous support and understanding throughout this endeavor, I would not have been able to complete it. To my advisors Doug MacKinnon and John Gibson, I appreciate all that you did to help me through this process. Your efforts and guidance truly made this a success. To SPAWAR SCTD expert Stephanie Koontz, your knowledge and willingness to help me made this entire thesis possible. I would not have had this opportunity without your support. To Commander Drew Ehlers, Commander Pete Nilsen, and the hard-working crew of the proud destroyer USS Cole, I thank you for your willingness to put up with me and the stellar support that you provided during my embarkation for this research. And finally, to the Distributed Information Systems Experimentation (DISE) group and those involved with making TRIDENT WARRIOR 2011 a success. Your tremendous effort to support the warfighter by bringing technological advancements to the Fleet is admirable.

THIS PAGE INTENTIONALLY LEFT BLANK

# I. INTRODUCTION

## A. INTRODUCTION

The speed with which information becomes available to a commander and his staff in the modern combat environment dictates that they have access to this information when, and where, it is required. Command and control (C2) by today's embarked commanders requires timely and reliable access to classified data systems at the C2 node provided by the ship. Most often, the spaces provided to an embarked staff are inadequate to support the commander's C2 requirements. Frequently, there are not enough classified computers or classified Local Area Network (LAN) connections to support the commander or his staff cells. An even greater challenge is when there are no available connections to allow classified connectivity. To facilitate some ability to exercise C2, a ship's company technicians will routinely place a hub on the network to provide extra connection points. This procedure takes time for the technicians to implement, as they must attempt to physically connect to the SIPRNet. With most spaces on a ship not serviced by existing SIPRNet connections, this requires running network cables through cableways from remote spaces. Even with this solution, there are still many spaces onboard that could not be serviced by running cables, as the nearest access to SIPRNet is farther than the maximum distances allowed by network cabling. A potential alternative may be to leverage current IEEE 802.11 technology to provide wireless connectivity for these clients.

## B. OVERVIEW

Use of a wireless solution in a shipboard environment has been employed in a small number of implementations since 2009 [1], and with the Consolidated Afloat Networks and Enterprise Services (CANES) program, every surface combatant in the U.S. Navy will have a working unclassified wireless LAN installed [2]. The current wireless LAN implementations are proving to be successful for mobility within the ship. Personnel become more efficient as they can move around while maintaining

connectivity with Personal Digital Assistants (PDA) and laptops. The current shipboard wireless network configuration is implemented as an extension of the ship's Non-classified Internet Protocol Router Network (NIPRNet) [1]. Classified connectivity for Secret Internet Protocol Router Network (SIPRNet) clients could be provided in much the same manner. However, running a separate wireless network to support SIPRNet connectivity would not only be costly in terms of implementation and maintenance, but would incite concerns of security and interference. One method however, demonstrates promise as a means to accomplishing the goal of transporting classified data across unclassified lines. This method is *tunneling*.

Tunneling encrypted SIPRNet data across the NIPRNet wireless extension is feasible through the use of either a KOV-26 (Talon) or a KIV-54 (SecNet54), both of which are NSA approved Type I encryptors. The concept to tunnel SIPRNet data across a NIPRNet was tested onboard USS Cole (DDG-67) during exercise TRIDENT WARRIOR 2011 (TW11), utilizing both the KOV-26 and the KIV-54 in the technology demonstration. Based on the results of the performance of SIPRNet clients observed using each of these devices, we intend to assess the potential this technology exhibits to support an embarked staff and its C2 requirements.

Additionally, we intend to address a secondary requirement of handling this classified data when it resides on the SIPRNet host. Data when not in transport or being processed by the host, but in storage for future use, is said to be data-at-rest. This data must also be protected, whether through physical or cryptographic means. Data-at-rest on an SCTD-enabled host must be protected to maintain the confidentially of that data.

### C. CHALLENGE OF SUPPORTING C2 REQUIREMENTS OF AN EMBARKED COMMANDER

Command and Control (C2) between an embarked commander and his subordinate units is challenging when the embarked platform is not configured to support the classified information requirements of the commander and his staff. Through the implementation of a wireless tunneling solution, greater flexibility will be afforded to both the embarking staff and the ship's company to support Command and Control (C2)

requirements in the spaces to which the staff is assigned. Study of the *tunneling* of SIPRNet data over a NIPRNet wireless network is required to validate the potential for a permanent classified wireless implementation.

## D. SCOPE

Although C2 is not necessarily limited to a technology problem, the proper application of technological solutions as an enabler of C2 is vital to maximizing the speed of command as it pertains to the six elements of C2. Admiral Willard, current commander of U.S. Pacific Command, defines the six elements of command and control as 1) maintain alignment, 2) provide situational awareness, 3) advance the plan, 4) comply with procedure, 5) counter the enemy, and 6) adjust apportionment [3]. These elements are better served by a responsive system of information flows, contributing to the speed of command.

It is imperative that the speed of command is faster than that of our adversaries, allowing U.S and Allied commanders to be opportunistic while forcing the enemy to be reactionary. These outcomes are dependent upon the receipt of timely and accurate information, the rapid processing of that data, and the fast promulgation of intent and taskings. The intent is to enhance the commander's ability to exercise C2 of assigned forces from locations that may not necessarily be equipped to support his requirements. It is in this information domain and its effect on C2, that this thesis focuses.

## E. METHODOLOGY

The design of this research centers around the implementation of two wireless tunneling technologies used in conjunction with an installed, functional wireless LAN onboard a U.S Navy warship. The methodology employed for this thesis consists of a literature review—including examination of operator surveys from previous experiments—operator surveys and subject-matter expert (SME) observations during TW11. An analysis of the data collected by using an unclassified wireless LAN to *tunnel* classified data, can demonstrate whether employment of either, or both, technologies adds value to the C2 nodes established by an embarked commander. Based on the results

of the surveys and observations, a recommendation will be made considering a permanent tunneling solution that may be implemented across the fleet.

## F. THESIS INTENT

The installation of unclassified wireless LANs on all surface combatants under the CANES program will ensure that all combatants will have an 802.11 wireless network onboard. However, it is installed to support unclassified requirements and will not address access to classified data. To enhance an embarked commander's ability to exercise command and control of assigned forces in any space throughout his flagship, the wireless LAN must be exploited to allow access to classified information. Without access to the classified networks, operational and tactical situational awareness cannot be maintained in many spaces throughout the ship that are not served by the wired classified network. Use of Secret Client Tunneling Devices (SCTDs) will provide the commander and his staff access to the classified network throughout the ship. It is this capability that is the focus of this thesis.

By applying survey research, an understanding of an enhanced C2 capability to support embarked commanders of afloat units may be ascertained.

This thesis will answer two questions:

- How can Command and Control (C2) requirements of an embarked commander be enhanced by using a KOV-26 (TALON) or KIV-54 (SecNet54) enabled SIPRNet laptop to *tunnel* data over an unclassified wireless connection?
- How can the Type I encryption, or Suite-B technology, be used to address data *tunneling* and data-at-rest at the SECRET level?

## G. ORGANIZATION OF THESIS

This thesis is organized into the following five chapters:

Chapter I frames the problem set that the thesis will address. Chapter II provides background information that is important to understand as it applies to the problem set.

This chapter discusses the history of 802.11 wireless Local Area Networks (LAN) and its use in the shipboard environment.  It further describes the tunneling technologies that were demonstrated during the TRIDENT WARRIOR 2011 (TW11).  Chapter III defines the measured figures of merit.  These figures of merit include 1) *usability*, the perceived latency, or responsiveness, of the system, and the ease of use with which an untrained user can setup the device, manipulate data found on the network external to the host, and securing the system for storage; 2) *availability*, a measurement of the accessibility of the network and the services that it provides to the user; and 3) *persistence*, the consistency with which a network connection is maintained.  It presents the methodology used to collect the data during TW11, and a detailed analysis of that data.  Chapter IV assesses the constraints and operational utility of extending the classified network as a method to enhance C2 capabilities of an embarked U.S. or Allied commander and his staff.  It also makes the distinction between each SCTD as to how they would most likely be employed in an operational context.  Chapter V, the final chapter, provides the conclusions made based on the research and offers some suggestions for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

# II. TECHNOLOGY REVIEW

## A. WIRELESS NETWORKING

In 2006, the Department of Defense (DoD) and the U.S. Navy authorized the use of wireless networking technology throughout the Global Information Grid (GIG). In October 2006, the Deputy Chief of Naval Operations Command, Control, Communications, Computers, and Intelligence (C4I) (OPNAV N6) transmitted NAVADMIN 06/283 that provided additional guidance for the implementation and installation of wireless networking components. Throughout this message, security is mentioned as a major factor for consideration of a Wireless LAN (WLAN) implementation.

> All WLAN traffic shall be protected by Federal Information Processing Standards (FIPS) 140–2 certified devices or technologies that authenticate and encrypt at or below Layer 2 of the Open Systems Interconnection (OSI) reference model. While some of the guidance cited herein may identify encryption at a higher OSI layer as being acceptable, the Navy DAA shall only accept solutions that provide encryption at layer 2 or below. [4]

Although at first glance this policy appears to fall short of what one would expect to be issued as guidance for protecting data, the requirement stems from the unique aspects of wireless LAN technology as compared to wired technology. Network security approaches for unclassified, wired networks make the assumption that the wired LAN connection is secure. As a result, security mechanisms concentrate on layer 3 and above. The Navy's approach to integrating commercial WLAN technology into the enterprise architecture is to secure the components of the network that directly pertain to the wireless portion of the wireless LAN to make it as secure, or more secure than that of a wired LAN. It is this thinking that dictates a focus on securing the network at layer 2. It is also required that the wireless client device will be maintained under the same configuration controls that apply to wired LAN devices for information assurance and security [5].

Further, NAVADMIN 06/283 discusses the use and storage of classified information over the wireless network.

> Wireless devices shall not store, process, or transmit classified information unless using assured channels employing National Security Agency (NSA) approved Type-I encryption. Type-II (FIPS 140–2) encryption is not certified by NSA and is not authorized for protecting classified information. [4]

The Navy has completed considerable testing of afloat WLAN technologies since this message was promulgated in 2006. In 2007, USS Cole (DDG-67) became the first Navy warship to have a functioning wireless network. Since then, several ships including USS George H. W. Bush (CVN-77), USS Howard (DDG-83), and HSV-2 SWIFT have had unclassified wireless networks installed. Additionally, USS San Antonio (LPD-17) has WLAN coverage throughout its superstructure, including its "well-deck" [6] from where its landing craft are launched.

Although security and frequency interference are considerations that must be addressed when installing WLAN on a warship, there are several benefits to having an unclassified wireless network installed. These benefits include mobility, cost savings, and installation flexibility [7].

Mobility as a benefit of a wireless LAN is defined as a user being able to access real-time information no matter where the user is located in the network. This mobility enhances the user's ability to efficiently perform his job requirements, and provides greater flexibility than that of a wired network [8]. As an example, a technician who is working on a faulty towed array sonar in the Tactical Towed Array Sonar (TACTAS) room onboard a DDG will have to access electronic documents that are embedded in the sonar suite in the forward—and remote—part of the ship, but has no computer access in TACTAS. With a wireless LAN, the technician can be able to access information stored on the network to help him complete repairs in the space where he is working. If the technician requires technical assistance to complete the repairs, a wireless classified computer can provide access to chat to allow near real-time communications with a technical representative ashore.

The cost savings that a wireless LAN provides is a true benefit. Although there is an initial investment associated with the wireless hardware and its installation, the overall cost of ownership and life cycle costs are dramatically lower than that of installing wired network switches and penetrating bulkheads to run network cabling as temporary requirements necessitate [8]. Once a wireless LAN is installed with adequate coverage throughout the ship, it costs virtually nothing to extend the network to spaces that do not have wired coverage.

Having flexibility with the installation of network connections in a location where those connections would provide value is a tremendous benefit [8]. Often when a staff embarks a ship, the spaces that ship provides the staff do not have the required number of network connections to adequately support the staff. In order to support the staff, a ship that is not configured with a wireless LAN will split an existing connection with a hub to support the staff. In cases where the space the staff has been given has no connections, the ship's technicians must run cabling from an existing connection through bulkhead stuffing tubes or watertight doors. A wireless LAN provides the flexibility to have required computer systems wherever the staff needs them.

### 1. 802.11b/g

The Wireless Local Area Network (WLAN) standards evolved from the first standard created by the Institute of Electrical and Electronics Engineers (IEEE). Initially created in 1997, the IEEE 802.11 standard has evolved through much iteration, and continues to grow today as the requirements for greater data capacity and increased speed-of-access to that data are demanded by the consumer [9].

To address the improved data and speed requirements, the 802.11b standard was published in September 1999. This standard defined three physical layers designed to provide different data rates, using the Industrial, Scientific, and Medical (ISM) 2.4 GHz band. The physical layers that it defined are Frequency Hopping Spread Spectrum (FHSS), Direct Sequence Spread Spectrum (DSSS), and Infra-red (IR) [9]. Although all three are still defined, the IR definition never gained in popularity, and is not a viable option for LAN connectivity due to lack of commercial products.

Both FHSS and DSSS were defined in the original 802.11 standard, but each only provided for a data rate of 1 or 2 Megabits per second (Mbps). In the 802.11b standard, not only does it define DSSS to ensure compatibility with devices produced to the 802.11 standard, but it also defines High Rate-Direct Sequence Spread Spectrum (HR-DSSS), with data rates of 5.5 and 11Mbps. This improved data rate, coupled with its compatibility with previous 802.11 DSSS devices, propelled the 802.11b standard to the forefront of popularity, and its implementation became the most common version of the WLAN standard of its time [10]. As improved versions of the 802.11 standard became further defined, they provided backwards compatibility to the 802.11b defined devices.

Although 802.11b is popular, it still does not provide a spectacular data rate. As consumers demanded more capacity, the IEEE continued to refine the 802.11 standards to meet that demand. In 2003, an amendment was ratified that defined the 802.11g standard. This standard implemented the use of Orthogonal Frequency Division Multiplexing (OFDM) at the 2.4GHz ISM band, and provided for data rates up to 54Mbps. Since 802.11g works in the same ISM band as that of 802.11b devices, it provides interoperability between the two standards, allowing consumers that have made considerable investment into an 802.11b WLAN to maintain their current infrastructure while upgrading key nodes of their network to 802.11g devices [9].

## B. SECURE CLIENT TUNNELING DEVICE (SCTD): KOV-26 AND KIV-54 DESCRIPTIONS

### 1. KOV-26 Talon Description

The first of the Secure Client Tunneling Devices (SCTD) considered for purposes of this thesis is the KOV-26 Talon, a National Security Agency (NSA) approved Type I encryptor that allows users to access data up to a level of Top Secret/Sensitive Compartmented Information (TS/SCI) that is developed and marketed by L3 Communications. It is designed as a multi-interface High Assurance Internet Protocol Encryption (HAIPE) device in a Personal Computer Memory Card International

Association (PCMCIA) form factor. It can provide classified data communications via an 802.11b or 802.11g WLAN, wired Ethernet, V.90 modem, or an RS-232 connection [11].

The Talon card is considered a Controlled Cryptographic Item (CCI) when it is not inserted into a designated laptop, and an authenticated user or Site Security Officer (SSO) is not logged onto the Talon Host Software (THS). It remains CCI when inserted into a designated laptop, as long as no authenticated user or SSO logs onto that THS[11]. As CCI, it is considered unclassified, but must be controlled as an accountable item [12]. When the Talon card is inserted into an authorized computer, and an authenticated user or SSO is logged into the THS, then the device becomes classified to the level of the keying material installed in the Talon. To return the Talon card to the state of a CCI, the authenticated user or SSO must either log out of the THS, or they can simply remove the Talon card [13].


Figure 1. The Talon and Its Tactical Kit Accessories. From [11].

The KOV-26 Talon card provides for up to 15 users per card. This can be one user per card on 15 configured laptops, 15 users on one laptop, or a combination not to exceed 15 (i.e., five user accounts on three different laptops.) As it is configured, the

Talon can only support one user logged on to one computer at a time. Although the Talon provides greater portability than the SecNet54, it does not provide bulk encryption for multiple computers simultaneously.

The value of the Talon card is its portability—its ability to take a classified laptop throughout the ship and allow classified network access in any space that has NIPRNet connectivity, whether by 802.3 Ethernet network connections or by an 802.11b/g WLAN. In the case of an embarked DESRON commander, the Commodore or his designated staff members can have classified access in multiple spaces throughout the ship. As an example, the Staff TAO (STAO) stationed at a location in the Combat Information Center (CIC), which does not have classified computer access, can be augmented by a Talon enabled classified computer. This would allow the STAO to access his required Command and Control (C2) applications, such as chat, e-mail, and the Collaboration At Sea (CAS) portal. The STAO and the Commodore can now exercise C2 of assigned forces from virtually any location on the ship.

### 2. KIV-54 SecNet54 Description

The second SCTD considered for this thesis is the KIV-54 SecNet54, a product line of bulk encryptors that provides access to both wireless and wired networks, depending on the modules that have been installed. It is an NSA approved Type I cryptographic device certified to handle data traffic up to TS/SCI. The SecNet54 is made up of the cryptographic module and a choice of external modules. The external modules available for the SecNet54 are the Radio module (RMOD), which allows a connection to 802.11b/g networks, and the Ethernet module (EMOD), which provides for connectivity to 802.3 wired networks [14].

The SecNet54 is handled as CCI prior to a user or administrator activating a key through an SSL certificate secured web application. Its classification is set by the administrator through this web application and it only activates keys compatible to that security classification level [15]. Figures 2 and 3 demonstrate the SecNet54 crypto

module (CMOD) and external Radio module (RMOD) or Ethernet module (EMOD) as both separate units and combined to make one operational unit, as a wireless interface device and as a wired device, respectively.

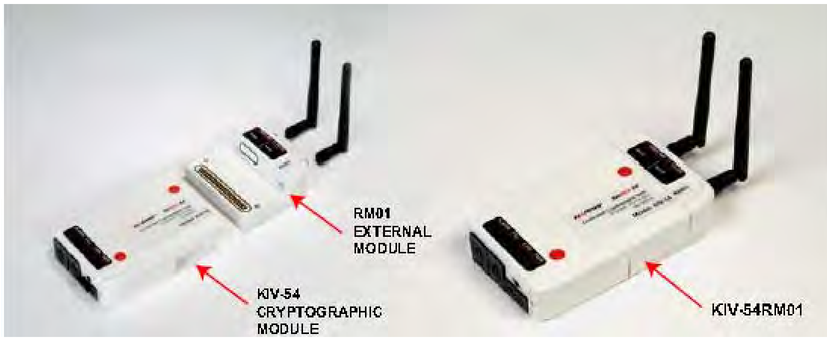



Figure 2. SecNet54 Cryptographic Module and Radio Module. From [16].

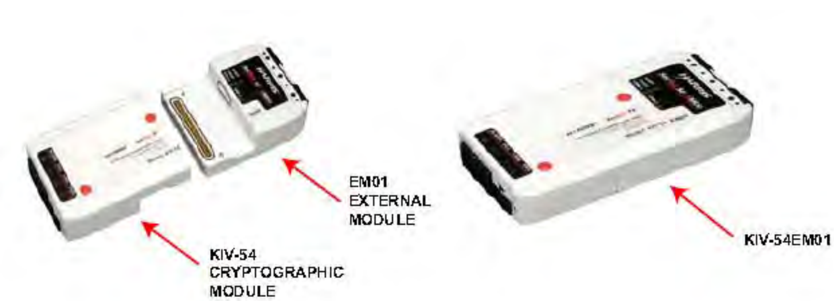



Figure 3. SecNet54 Cryptographic Module and Ethernet Module. From [17].

The SecNet54 does require an external power source. Power can be provided from an included power supply, battery power, or it can be provided by an 802.3af Power over Ethernet (PoE) device [16]. The power options of the SecNet54 make it less portable than the KOV-26, which receives its power from the host laptop.

To connect classified computers, the SecNet54 can be plugged directly into a computer or a switch. By attaching a commercial off-the-shelf (COTS) switch to the SecNet54 by way of an ethernet connection, the administrator is able to have multiple

hosts attached to one SecNet54 device, creating a classified enclave. The true value of the SecNet54 is being able to create an enclave of multiple computers in a space that does not have classified network access. Figure 4 shows a single SecNet54 connected to a Cisco switch to provide multiple hosts access to the tunneling device.

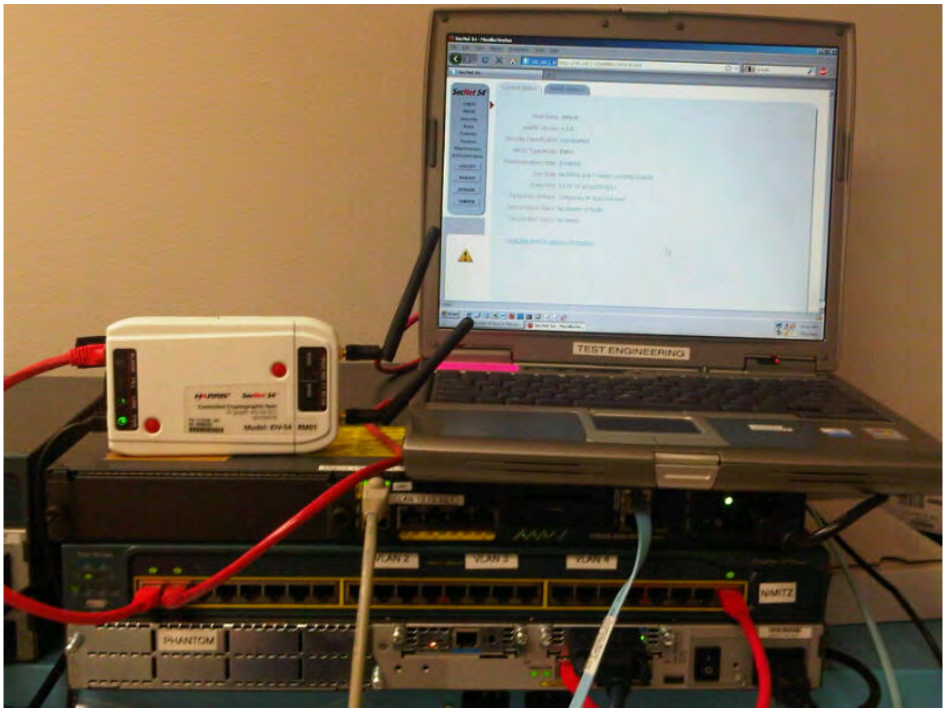



Figure 4. SecNet54 Radio Module Providing Tunneling Services to Switch.[1]

In order to support an embarked commander, the SecNet54 can be used to create a classified workspace for his staff in a space that has at least one NIPRNet connection or is serviced by a NIPRNet wireless LAN. In the case when a DESRON commander embarks on a DDG, the staff is most often given the classroom as its workspace. On most DDGs the classroom has one or two NIPRNet connections with no available SIPRNet connections. By installing the SecNet54 into a NIPRNet connection utilizing the EMOD and using a COTS switch, the classroom becomes a classified workspace for the staff by providing multiple classified computers with classified network access.

[1] Photo courtesy of Mr. Paul Johnson, Harris Corporation systems engineer.

## C. SUITE-B/FIPS140–2 COMPLIANCE IMPLICATIONS AND SHORTFALLS

FIPS140–2 specifies the security requirements for a cryptographic module utilized within the security system protecting sensitive information in computer and telecommunication systems. These security requirements are defined for separate security levels. Security Level 1 is the minimum security requirement. Basic security requirements, such as utilizing at least one approved algorithm or approved security function, are specified. Additionally, Security Level 1 does not require specific physical security mechanisms [18].

Security Level 2 enhances the physical security mechanisms by adding the requirement of tamper-evidence, such as tamper-resistant seals or pick resistant locks placed on doors or removable covers. This protects the device against unauthorized physical access, and makes it apparent when unauthorized access has been attained. Additionally, Security Level 2 requires role-based authentication in which a cryptographic module authenticates the authorization of an operator to perform a specific role and that role's service set [18].

Security Levels 3 and 4 provide increasing security requirements, respectively, with Level 4 providing the highest level of security in the FIPS 140–2 standard. Level 4 cryptographic modules are best utilized for operations in physically unprotected environments [18]. Although attainment of Level 3 or Level 4 is desired, the increased costs associated with that attainment is not justified in the physically secure environment of a Navy warship.

As described in NAVADMIN 06/283, wireless networks must comply with FIPS140–2 Level 1, and the transfer of classified data over the wireless network must be encrypted with Type-I bulk encryption. The wireless networks currently fielded by the U.S. Navy are comprised of 3eTI wireless network devices which are certified FIPS140–2 Level 2 compliant. Devices that wish to access this wireless network must be mutually authenticated using the Extensible Authentication Protocol-Transport Layer Security

(EAP-TLS) [4]. This security method addresses the access to the unclassified network by authorized devices. The method does not address confidentiality of classified data.

As discussed previously, the KOV26 and KIV54 provide NSA Type-I bulk encryption of classified data, up to TS/SCI, which allows that encrypted data to be transported on an unclassified network. However, most requirements for the KOV26 and KIV54 are for data that is classified at SECRET or below, which makes this type of encryption suitable for consideration of Suite-B devices [19].

NSA is moving toward Suite-B cryptography as an answer to the need for the secure sharing of information down to the tactical user up to the SECRET level. To satisfy this requirement, NSA feels that approved information assurance solutions must be widely available and affordable for the user. As a result, the NSA has initiated three efforts to meet these objectives:

1. The Cryptographic Interoperability Strategy

2. Expanding the use of GOTS products that meet a revised set of security standards to protect information up to the SECRET level; and

3. Layered use of COTS products that meet a more robust set of security standards to protect information up to the SECRET level. [19]

Suite-B is being designed to complement existing policy regarding the use of the Advanced Encryption Standard (AES), which protects national security information systems and the data that resides on most systems. Suite-B includes cryptographic algorithms for hashing, digital signatures, and key exchange [20].

The main aspect of Suite-B Cryptography is its use of elliptic curve technology instead of traditional public key technology. There are 26 patents held by Certicom, Inc., that the NSA has licensed rights for the use with respect to the Suite-B elliptic curve technology. To facilitate the utilization of Suite-B by commercial industry, NSA's license includes the right to grant a sublicense to vendors building certain products or components that can be used for protecting national security information [19].

## D. CAPABILITIES

The benefits of implementing an SCTD architecture are the same as the benefits of implementing a wireless LAN afloat. In fact, SCTD provides mobility, cost savings, and installation flexibility, all at the classified data level. It is at this level that command and control (C2) by a commander of assigned forces resides. As commanders and their staffs move from ship to ship, and as their C2 nodes change configuration based on the ship-assigned space in which the commander and his staff work, it is incumbent on the ship to comply to the information protection requirements dictated by the commander and established policies. By using either SCTD solution, whether over a wired or wireless network, C2 of assigned forces will be enhanced by this extension the classified network.

For SCTD usage to be successful, it cannot introduce latency to the command and control equation. Both the KOV 26 and the KIV 54 introduce no significant latency, and in some cases improve noticed latency. By tunneling through a robust unclassified network, the ideal situation is that the user notices very little difference between working on the ship's classified network–a desktop computer attached to a standard configuration network connection–with that of working with an SCTD extended laptop. This capability will not only enhance the C2 of U.S. Navy commanders, but will enhance the C2 requirements of coalition commanders and sister-service combat elements, such as embarked Marine units, on U.S. Navy vessels.

Further, the fleets of the U.S. Navy are each tasked to conduct Theater Security Cooperation operations with coalition partner nations. Such engagement activities often come in the form of mutual exercise participation, in which the coalition partner embarks a United States ship to act as the commander of assigned forces. This requires that commander and his staff the ability to conduct command and control from the spaces the ship provides. The SCTD can be used to extend the classified coalition network to these spaces. As an example, either SCTD could be keyed with the CENTRIXS key, and moved to any space on the ship.

## E. CONSTRAINTS AND LIMITATIONS

Although use of an SCTD has great potential for enhancing command and control of an embarked commander by extending the classified C2 network, there are policy limitations that govern the use of these classified devices.

A limitation to using the SCTD, especially with coalition partners, is the accountability requirements for a device at a classification level or at rest as a CCI device. When either the KOV26 or the KIV54 is logged on by an authorized user or SSO, the SCTD and enabled client is classified to the level for which the data is keyed [11], [15].

As both SCTDs are designed for bulk encryption of data across the transport layer, they do not address the classification of the data at rest. As data is being generated or retrieved on the client device, it is being stored on that client. This requires strict adherence to Department of Defense and Department of the Navy physical security and Information Assurance (IA) policies. It is also pertinent to point out that, although an organization can extend the classified network through use of SCTDs, care must be taken as to where the network is extended. Even though a user has the capability to use an SCTD enabled client in an otherwise unclassified space, such as on the mess deck, the user must be aware of his surroundings. It is possible that a Sailor who does not possess a clearance may be able to shoulder-surf to gain classified information. The ease with which an SCTD can be used may actually increase the potential for this kind of exploit.

This chapter has discussed the principles of wireless LAN technology and its related security as required by DoD and DON instructions. It also provided background on the KOV26 Talon card and the KIV54 SecNet54, NSA approved Type-1 encryptors that allow the tunneling of classified data across an unclassified wired or wireless network. It is these devices that were demonstrated during Trident Warrior 2011 (TW2011) onboard USS Cole to qualitatively determine the usability and persistence of connection of both devices on an afloat wireless LAN.

# III. DATA COLLECTION AND ANALYSIS

## A. TRIDENT WARRIOR 2011 (TW11)

### 1. Exercise Overview

Trident Warrior (TW) is an annual fleet experiment designed to improve warfighting policies and capabilities by providing answers to detailed analytical questions about more than 50 critical maritime initiatives included in the experiment's execution. TW11 provided an organized and streamlined venue to experiment with many possible solutions to the Fleet's current and future challenges, resulting in consistent in-depth analysis to Navy's decision makers. TW11 included at-sea experimentation of initiatives and developing or improving tactics, techniques, and procedures (TTPs) to aid maritime forces; encompassing all aspects of the modern warfare spectrum—air, land, sea, and cyber. For 2011, Trident Warrior was conducted in the SECOND Fleet and FIFTH Fleet Areas of Operations (AO) [21]. The studies outlined in this thesis occurred from July 25 to August 1 during the SECOND Fleet portion of TW11.

### 2. Secure Client Tunneling Devices (SCTD) Technology Demonstrations

TW11 marked the second time the KOV-26 was demonstrated on an afloat wireless network. It was tested previously on USS Bonhomme Richard (LHD 6) during Trident Warrior 2010 (TW10) in the THIRD Fleet AO. During TW10, the wireless network used to evaluate Talon was installed specifically for TW10. Although it was considered successful, with the Talon demonstrating the ability to provide a usable and persistent connection to SIPRNet, it did not truly test the connection through a ship's organic wireless LAN.

During TW11, the KIV-54 was added to the testing of SCTDs. Both the SecNet54 and the Talon were tested to demonstrate a usable and persistent connection over an organic afloat NIPRNet-hosted wireless LAN. The demonstration was conducted aboard the USS Cole. By the very nature of testing on a fielded WLAN at sea, the intent

of the demonstration was to definitively prove that there is value in fielding the KOV-26 or the KIV-54, or both, to enhance C2 resource access by an embarked commander.

To connect either SCTD to USS Cole's wireless architecture, a KG-175D was installed in the Radio Room onboard the Cole. The KG-175D is an encryption device that handles the encrypted packets from the Talon or the SecNet54, acting as the bridge between NIPRNet and SIPRNet traffic. Once the KG-175D received the encrypted packets from the NIPRNet, it decrypts those packets and injects them on the SIPRNet. When the Talon or SecNet54 supported device was to receive data, the KG-175D would handle packets in the reverse order—receive the classified data from the SIPRNet, encrypt it, then transmit the encrypted packet on the NIPRNet to the recipient SCTD. The architecture for both devices are depicted in Figures 5 and 6, respectively. The primary difference between the architectures is the ability of the SecNet54 to provide access to an enclave of hosts rather than a single remote host.

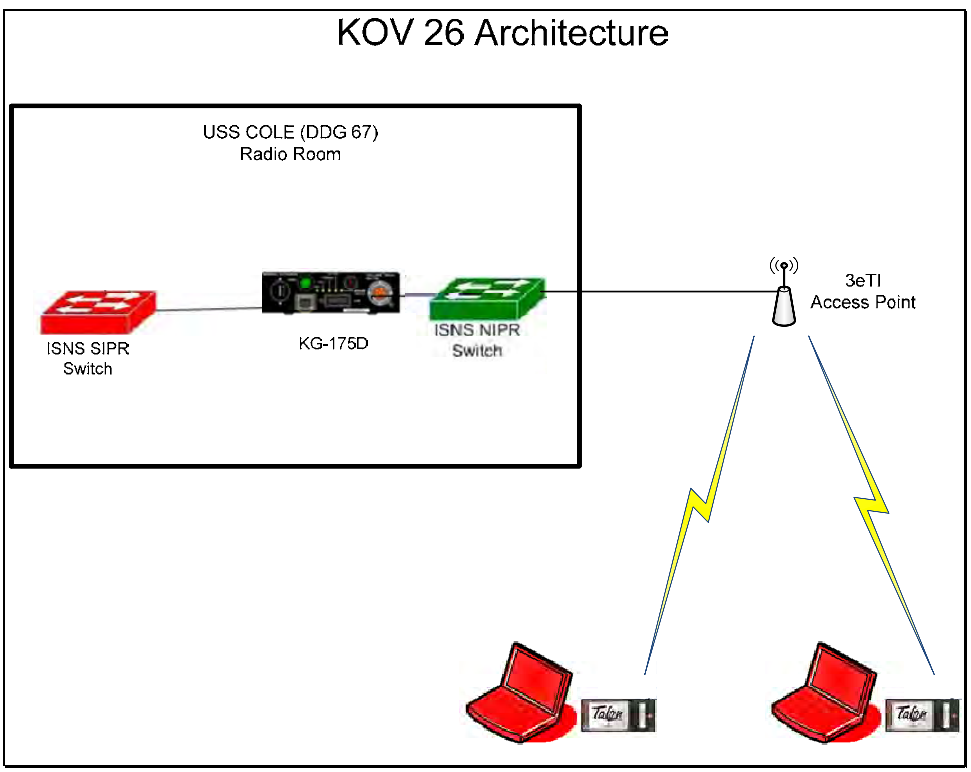



Figure 5. USS Cole (DDG67) KOV-26 Architecture for TW11. After [22].

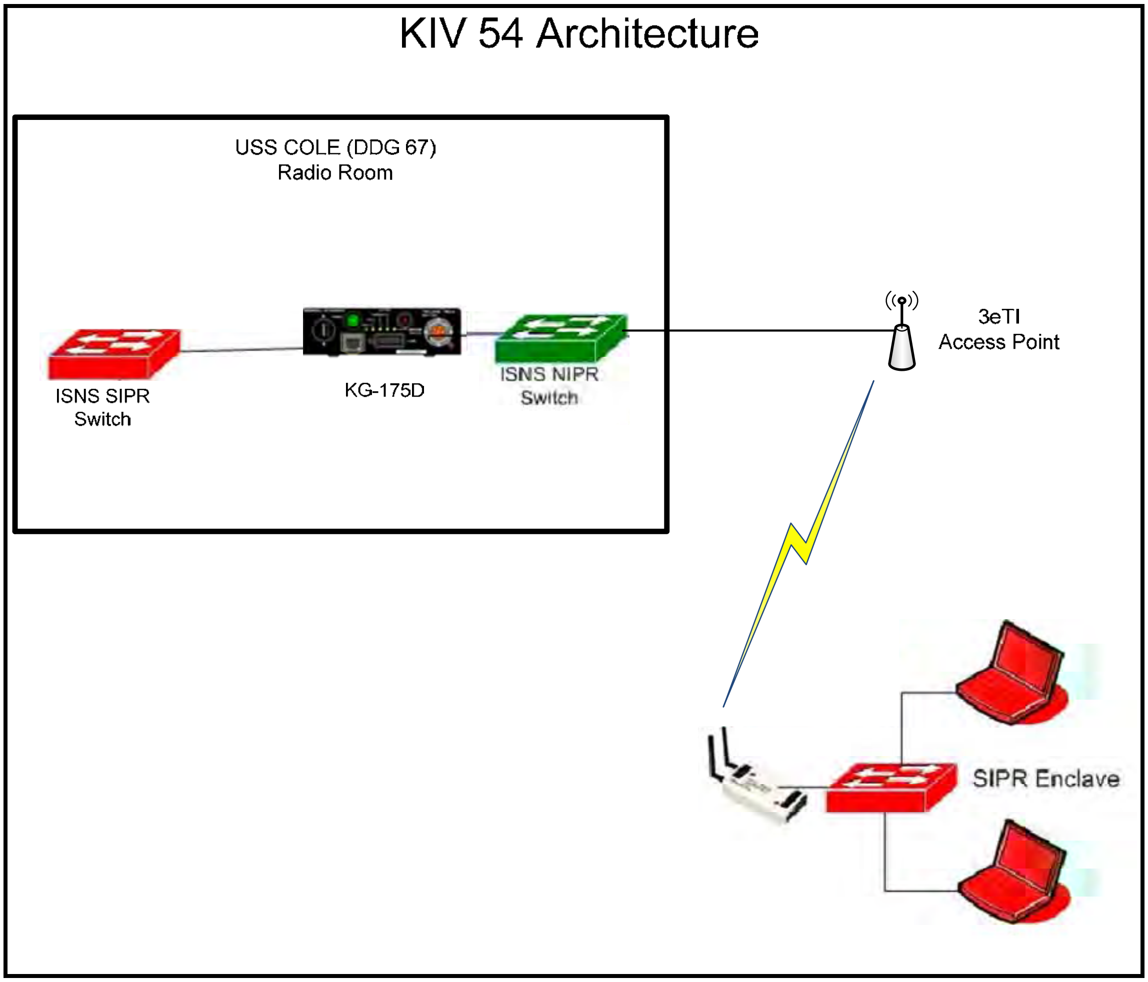



Figure 6. USS Cole (DDG-67) KIV-54 Architecture for TW11. After [22].

## B. DATA COLLECTION AND ANALYSIS

### 1. Evaluation Criteria and Methodology

The TW11 SCTD evaluations were designed to determine three measures; usability, availability, and persistence. Usability was defined as the perceived latency, or responsiveness, of the system, and the ease of use with which an untrained user can setup the device, logon to the user interface to establish the tunnel, manipulate data found on

the network external to the host, and securing the system for storage. It was measured in both SCTD Operator Surveys, with the resultant answers being converted to either a "Positive" or "Negative" answer.

The figure of availability was defined as the measure of accessibility of the network and the services that it provided to the user. For this study, the number of initial connection attempts and the users' problems, as articulated in the surveys, with using applications on the network were considered as measurement of this figure.

Persistence as a figure of merit was defined as the consistency with which a network connection was maintained. It was captured in the surveys by questions pertaining to the continuity of connection during the user's session.

The TW11 SCTD evaluation methodology consisted of the use of both operator surveys and Subject Matter Expert (SME) observations. A list of Cole authorized SIPRNet users were generated from Cole's SIPRNet Active Directory. Users were randomly selected as they became available between duty "watches," ship's drill evolutions, and other shipboard requirements. Users ranged from junior enlisted (E-3) to senior field grade officers (O-5). Once selected, each user was assigned a duty-position using either a KOV-26 or KIV-54 and its associated laptop. The user would also be provided a set of instructions that would guide him through the initial setup of the SCTD client and the required tasks to be performed. For the Talon, the operator would perform the required steps in sequence, as depicted in the Talon workflow diagram (Figure 7).

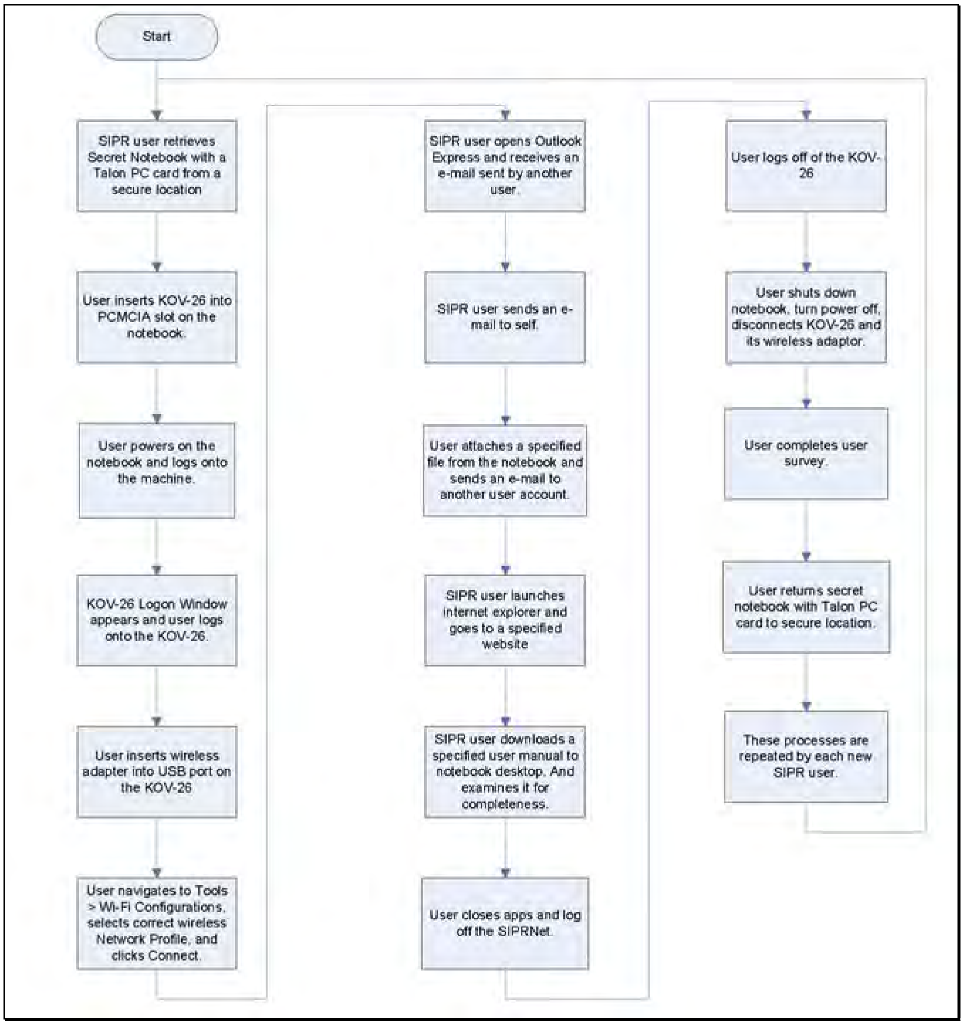
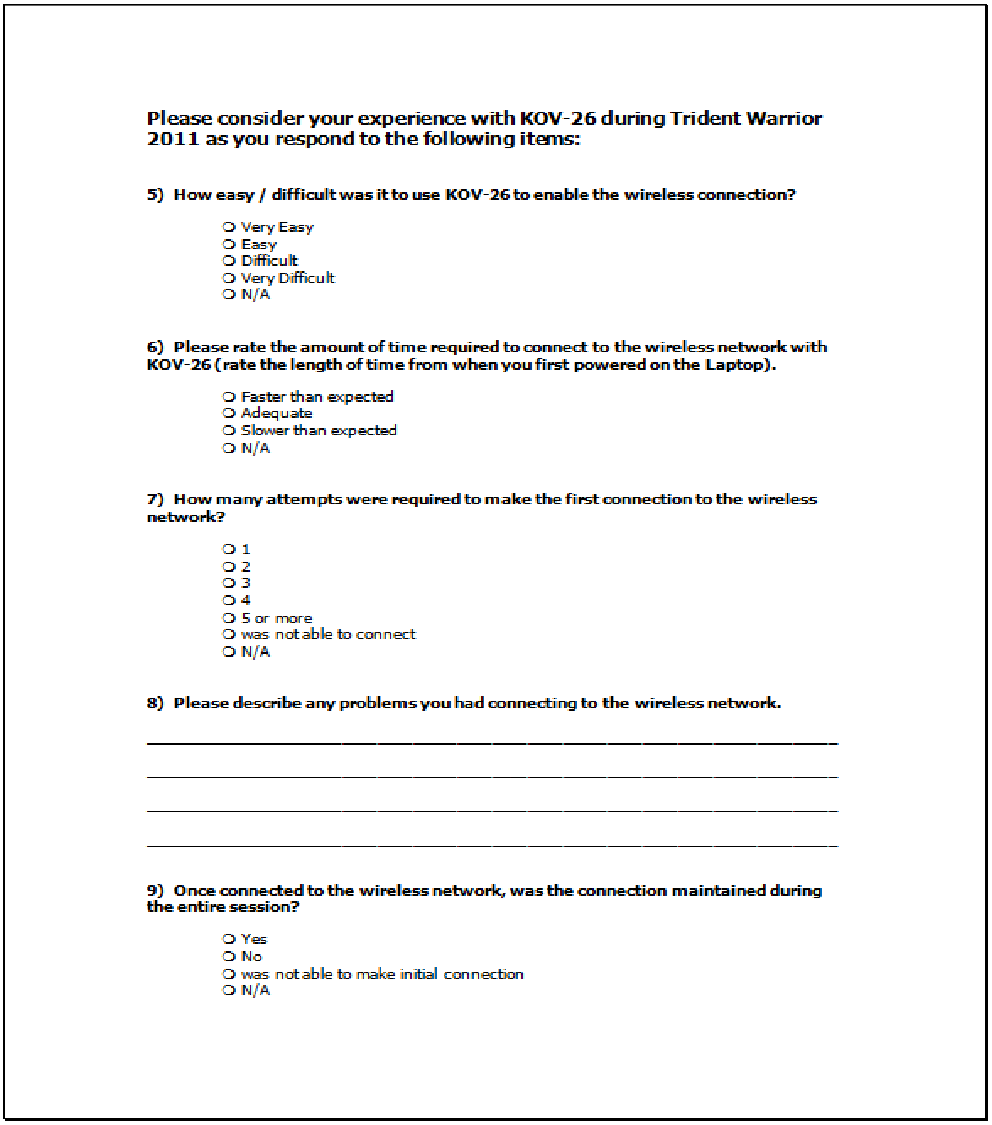



Figure 7. KOV-26 Workflow Diagram. From [23].

The tasks that the operator was to perform to demonstrate the usability of the system included e-mailing a file between users, opening a received file, and visiting an external website to download a large file (516 MB). These actions were intended to demonstrate to the operator any latency introduced as a result of the wireless network or because of the extra encryption/decryption process required by the tunneling. By having the user assess the latency of the tasks as compared to performing similar tasks on a standard SIPRNet host, the user would be able to provide a qualitative value of the usability and responsiveness of the remote access capability. As seen by the standard

user, latency is directly related to usability or responsiveness. An example of the questionnaire used to collect the survey data is provided in Figure 8. The full KOV-26 Operator Survey can be found in Appendix B.



**Please consider your experience with KOV-26 during Trident Warrior 2011 as you respond to the following items:**

**5) How easy / difficult was it to use KOV-26 to enable the wireless connection?**

- Very Easy
- Easy
- Difficult
- Very Difficult
- N/A

**6) Please rate the amount of time required to connect to the wireless network with KOV-26 (rate the length of time from when you first powered on the Laptop).**

- Faster than expected
- Adequate
- Slower than expected
- N/A

**7) How many attempts were required to make the first connection to the wireless network?**

- 1
- 2
- 3
- 4
- 5 or more
- was not able to connect
- N/A

**8) Please describe any problems you had connecting to the wireless network.**

______________________________________________

______________________________________________

______________________________________________

______________________________________________

**9) Once connected to the wireless network, was the connection maintained during the entire session?**

- Yes
- No
- was not able to make initial connection
- N/A

Figure 8. Portion of KOV-26 Operator Survey. From [24].

Throughout the completion of the instruction sheet, the SME maintained the SME Observation Log, and would ask questions to get an idea of how the operator felt about the usability of the Talon-based access and his perception of the persistence or responsiveness of the SIPRNet connection. The user would continue through the end of

the Talon instruction sheet, which included the shutdown of the system as the final step. Upon completion of all steps, the user filled out the KOV-26 Operator Survey.

Having completed the Operator Survey for the KOV-26, the participant proceeded to the evaluation of the KIV-54. At this point, he was given another instruction sheet, this time for the SecNet54, and the procedure to be stepped through to accomplish the evaluation. Most of the steps were similar to those outlined in the KOV-26 instruction sheet, which included e-mailing, remotely accessing large files, and visiting an external webpage. In Figure 9, the workflow for the SecNet54 is depicted.

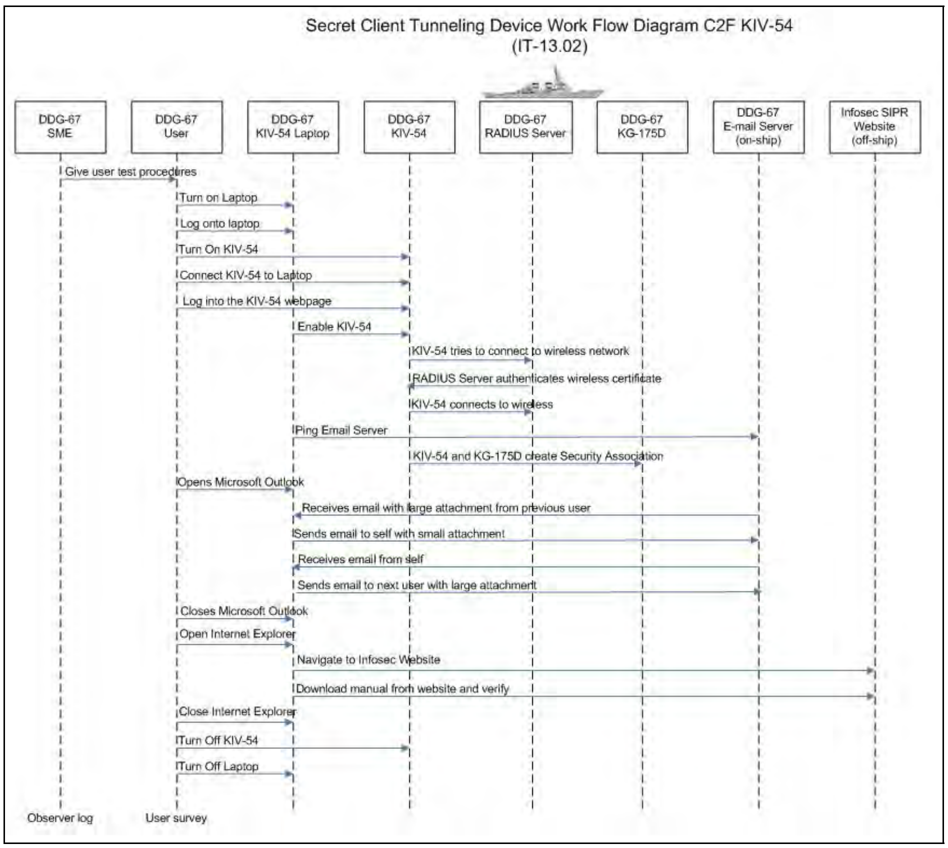



Figure 9. Workflow for KIV-54 Testing. From [25].

It is important to note that although several users started their testing period with the KOV-26, this was not required. Some users did start with the KIV-54, thereby finishing with the KOV-26. Although the surveys did not ask for the user to compare the

devices, it was a natural progression of the testing, and many users did make a comparison statement in their final survey. Additionally, some users made comments about the comparison between both devices to the SME that were captured in the SME Observation Log.

Throughout the completion of the instruction sheet, the SME maintained the SME Observation Log and would asks questions to get an idea of how the operator felt about the usability of the SecNet54 and their perception of the persistence of the SIPRNet connection. The user continued through the end of the SecNet54 instruction sheet, which included the shutdown of the system as the final step. Upon completion of all steps, the user completed the KIV-54 Operator Survey which is of similar form to that of the KOV-26 Operator Survey. The full copy of the KIV-54 Operator Survey can be found in Appendix B.

Although most of the data collection was taken while users were in either the Radio Room or the Operations Office, there were opportunities to demonstrate the connection-extension capabilities of both the Talon and the SecNet54 in spaces throughout the ship. These spaces included the Nixie Winch Room and the Tactical Towed Array Sonar (TACTAS) Room, both at the stern of the ship; the Wardroom, which had neither a NIPRNet nor a SIPRNet connection; the Bridge and Bridge Wings; and the Engineering Central Control Station (CCS). From all spectators of these demonstrations, the common response was to ask, "How do we get this capability permanently installed?" This was a clear indicator that they felt both devices show great potential to extend their SIPRNet access to otherwise un-serviced areas of the ship. This matched their sentiment—as articulated in survey responses and captured in the SME Observation Logs—that there were too few SIPRNet machines onboard to meet the required classified workload.

### 2. Analysis

The testing of both SCTDs took place over a period of six days, with the goal of engaging at least four authorized SIPRNet users per day, for a total of 24 users in the

sample. Actual sample size during TW11 expanded to 30 users. Of those users sampled, none had used either SCTD prior to their evaluation during TW11.

### *a. Usability*

Usability is directly related to the perceived latency of data which affects the user's completion of common tasks, such as sending or receiving e-mail, opening a website, or downloading a file. Usability was captured by asking questions related to the users' perception of the speed in which tasks were completed, with the scale being "Faster than normal," "About the same," "Slower than normal," or "N/A." Usability was also evaluated by the ease of use of the device. The grading scale for this criterion was "Very Easy," "Easy," "Difficult," "Very Difficult," or "N/A."

| | Question Type | Answer Evaluation | | | | | |
|---|---|---|---|---|---|---|---|
| Question | | POSITIVE RESPONSES | | NEGATIVE RESPONSES | | | NEUTRAL |
| 5 | Radio button | Very Easy | Easy | Difficult | Very Difficult | - | N/A |
| 6 | Radio button | Faster than expected | Adequate | Slower than expected | - | - | N/A |
| 12 | Radio button | Faster than normal | About the same | Slower than normal | - | - | N/A |
| 13 | Radio button | Faster than normal | About the same | Slower than normal | - | - | N/A |
| 14 | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | |
| 16 | Radio Button | - | No problems loading | Minor problems loading | Major problems loading | - | N/A |
| 17 | Radio button | Faster than normal | About the same | Slower than normal | - | - | N/A |
| 19 | Radio Button | - | No problems loading | Minor problems loading | Major problems loading | - | N/A |
| 20 | Radio button | Faster than normal | About the same | Slower than normal | - | - | N/A |
| 21 | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | |
| 22 | Radio button | Strongly Agree | Somewhat Agree | Somewhat Disagree | Strongly Disagree | N/A | |
| 24 | Radio button | Very Satisfactory | Somewhat Satisfactory | Somewhat Unsatisfactory | Very Unsatisfactory | N/A | |
| 25 | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | |

Table 1. Survey Criteria for *Usability*

To determine the actual usability figure of merit, the data was classified as a positive answer if the usability was at least the same as that of the usability of a ship's installed wired SIPRNet computer. From the scales listed above, that equated to "About the same" or better and "Easy" or better. All other assigned values were considered to represent a negative measurement. Table 1 displays the key used to determine whether

an answer is positive or negative. Both the KOV-26 and the KIV-54 scored well, with approximately 95% of the answers being positive.

### ***b. Availability***

*Availability* addresses the accessibility of the network and the services it provides. Values used to quantitatively measure *availability* include the number of attempts required to connect or reconnect to the wireless network, where a value of “1” is considered a positive answer, and a value of “2” or greater represents a disconnect with a subsequent reconnect, which is interpreted as a negative answer. Additional values provided by the users include “Yes” or “No” when asked if they were able to perform a task as outlined in the instruction sheet. Examples of these tasks include being able to use Internet Explorer to download a file or sending and receiving e-mail using Outlook. An answer of “Yes” was categorized as a positive answer and an answer of “No” was listed as a negative answer. Answers of “N/A” were treated as the user not performing the task for some reason. This value was treated as neither a positive nor a negative response in most instances. The one exception was in question 10, which asked “If the connection was lost during the session, how many times was it lost?” For this question, “N/A” was treated as a positive answer, and any numeric value was treated as a negative response. Table 2 provides the criteria of answers from the survey to determine whether the criteria are positive or negative.

The survey results confirm an overwhelmingly positive response, with 96% of the responses recorded for the KOV-26, and 97% of the responses recorded for the KIV-54 being positive.

| | Question Type | Answer Evaluation | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| **Question** | | **POSITIVE RESPONSES** | | **NEGATIVE RESPONSES** | | | | | NEUTRAL |
| **7** | Radio button | - | 1 | 2 | 3 | 4 | 5 or More | Was not able to connect | N/A |
| **10** | Radio button | - | 1 | 2 | 3 | 4 | 6 or More | Was not able to connect | N/A |
| **14** | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | | | |
| **15** | Radio Button | - | Yes | No | - | - | - | - | N/A |
| **18** | Radio button | - | Yes | No | - | - | - | - | N/A |
| **21** | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | | | |

Table 2. Survey Criteria for *Availability*

### *c. Persistence*

Although similar to availability, *persistence* pertains to the consistency of the network connection. This is simply measured by asking the user if they had any problem establishing and maintaining a network connection. This was recorded as the number of connection attempts performed, with "1" being the initial attempt, and anything greater than "1" represents a disconnect with reconnect attempts. Table 3 portrays the survey criterion used to determine the values of positive and negative persistence.

| | Question Type | Answer Evaluation | | | | | |
|---|---|---|---|---|---|---|---|
| Question | | POSITIVE RESPONSES | | NEGATIVE RESPONSES | | | NEUTRAL |
| **8** | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | |
| **9** | Radio Button | - | Yes | No | Was not able to make initial connection | - | N/A |
| **11** | Free text | Interpreted based on response. No response is considered positive. | | Interpreted based on response. | | | |

Table 3. Survey Criteria for *Persistence*

From the survey results, both the KOV-26 and the KIV-54 scored well among the users, with over 90% experiencing a stable, uninterrupted connection. Of those that reported having to reconnect the KOV-26, all were a result of a laptop malfunction, as indicated in the KOV-26 SME Observation Logs. For those that reported multiple connections for the KIV-54, it was determined to be an initial setup error, such as a duplicate IP address or a missing certificate that is required to access the web login application. Although this is an issue that should be identified under the usability metric, it manifested itself under the persistence metric.

### 3. Summary

This chapter discussed the methods used to determine usability of the SCTDs, the availability of the network and its associated services, and the persistence of the network connection. Further, it presented the analysis of the data. The operator survey results of the KOV-26 and the KIV-54 demonstrate that both devices provide a very *persistent* connection, and were considered very usable. Additionally, tasks that were facilitated by the KOV-26 Talon or the KIV-54 SecNet54 were readily *available*.

Chapter IV will analyze both SCTD solutions in the context of enhancing Command and Control (C2) for an embarked commander and his staff as we envision the devices to be employed. Considerations for the SCTD employment will also be discussed pertaining to network security.

THIS PAGE INTENTIONALLY LEFT BLANK

# IV. ASSESSING CONSTRAINTS AND OPERATIONAL UTILITY OF EXTENDING THE CLASSIFIED NETWORK

## A. OVERVIEW

From the previous chapter, one can see that both the KOV-26 and the KIV-54 provide value to the users of classified hosts. In almost all cases, the ease-of-use and persistent, reliable connection provided by both SCTDs were remarked to have provided great value to the ship as they were able to extend the SIPRNet throughout the ship. Additionally, the minimal cost and ease of installation of these SCTDs make fielding them a much more palatable proposition than that of fielding permanent classified network connections throughout the ship.

While the value of employing SCTDs over a NIPRNet wireless LAN has proven to be an operationally worthwhile venture, it is not meant to replace the current wired architecture of an afloat SIPRNet enclave. Classified network connections should still be utilized for access to network resources as a redundant, yet different path. The wired network is still an important part of a command and control node and must be maintained for full employment during times when RF communications are not possible.

The purpose of this chapter is to discuss the operational utility of fielding the SCTDs as a method of extending the ship's classified network in order to enhance the C2 capabilities as they apply to the embarked commander, both U.S. and allied. Further, the inherent risks associated with fielding an SCTD solution, and the mitigations to those risks are examined.

## B. OPERATIONAL CONSIDERATIONS

The KOV-26 Talon and the KIV-54 SecNet54 both provide wired and wireless extension of a ships classified network. Although both are similar in this respect, their scheme of employment is markedly different. The KOV-26 provides for better mobility than the KIV-54, in a much smaller form factor. However, the KOV-26 can be used for

only one device at a time, whereas the KIV-54 has the ability to connect multiple hosts in a single enclave. It is this distinction between the two devices that will dictate the operational use of either device.

Both SCTDs can be used to enhance command and control by embarked commanders and their staffs in spaces that either do not have the required number of classified connections or do not have any installed classified connections to address the communications requirements that support effective command and control at that C2 node. A summary of characteristics of both the Talon and the SecNet54 can be found in Table 4.

### 1. KOV-26

The KOV-26 Talon is best suited for individual access to network services such as file sharing, collaborative tools, chat, and e-mail—that is, a single host connecting to the classified network. Situations where the capability of this SCTD is ideal for an embarked commander include being able to maintain situational awareness of his assigned forces while roaming throughout his flagship. He would have at his disposal a Common Operational Picture (COP), e-mail and chat communications with his Staff Tactical Action Officer (STAO) and subordinate commanders, as well as his superiors.

Another example of where the KOV-26 Talon is beneficial to an embarked naval commander is in the case where Marines have embarked on an amphibious ship. With the ship having wireless LAN coverage throughout the superstructure, as well as in the well deck, Marines waiting to be launched from the well deck can sustain classified communications with their commanders to maintain situational awareness of the objectives of the amphibious assault. Additionally, the Marines standing by in the well-deck can transmit equipment status updates to the commander's staff, keeping the staff apprised of changes as they occur in near real-time. This same SCTD enabled host that connected to the ship's wireless LAN can then be used in forward operating areas by connecting to the wired or wireless LAN of the forward operations base.

To this point, we have only addressed the embarkation of a U.S. commander and his staff on a U.S. Navy vessel with SIPRNet as the required classified network. On

numerous occasions, however, the embarked commander and his staff may be that of a coalition partner to support a combined exercise or a coalition contingency operation. When these commanders and their staffs embark a Navy warship, they require access to several CENTRIXS computers. On U.S. Navy destroyers, the only CENTRIXS hosts are found in the Combat Information Center (CIC) or in the Radio Room. This does not provide enough access to classified releasable hosts for the commander, his STAO, or his staff.

Keying the Talon with the appropriate CENTRIXS key, the commander or his STAO, or both depending on the number of Talons available, will be able to access all collaboration tools and documents available on the CENTRIXS enclave, enhancing his ability to command and control not only his national forces, but the coalition forces as well. Through the use of an SCTD enabled CENTRIXS host, the commander can access message traffic, e-mails, documents and chat rooms that are common throughout the CENTRIXS enclave, thereby improving his speed of command.

| | KOV-26 | KIV-54 |
|---|---|---|
| **Powered by External Source** | No | Yes |
| **Powered by Host** | Yes | No |
| **Connects Multiple Hosts** | No | Yes |
| **Connects to Wireless LAN** | Yes | Yes |
| **Connects to Wired LAN** | Yes | Yes |
| **Can host a VoIP Phone** | No | Yes |

Table 4. SCTD Characteristics Comparison

### 2. KIV-54

The KIV-54 SecNet54 can provide access to classified data for a single host much like that of the KOV-26. However, the external power requirements of the SecNet54 make it much less mobile than that of the Talon. The value of the SecNet54 can be found

in its ability to create an enclave of multiple classified hosts from one SecNet54. Although not ideally suited for a single point C2 node, it can be used by a staff to support the commander and his C2 nodes.

Typical staff complements of an embarked commander include planning cells, operations cells, and intelligence cells, each of which has classified data access requirements. Continuing with the illustration of a commander and his staff embarking a U.S. Navy destroyer, the staff is generally assigned a space within which to work that may not meet these requirements. Examples of typical spaces assigned to the embarked staff are the classroom, which contains no more than two NIPRNet connections with no SIPRNet connections, or the Operations Office, which contains two SIPRNet connections and one or two NIPRNet connections. Neither space is adequate to support the needs of the staff and its different cells.

Adding a SecNet54 and a multiport switch to either space will address the requirements imposed by the staff. By creating a classified enclave in a single space, the staff and its cells will be able to work simultaneously, either independently or collaboratively at the same classification level. This increases the efficiency of the staff planning process by providing the needed access to classified information such as commander's intent promulgated via message traffic, intelligence fusion products, and current operational status depicted on a COP.

The SecNet54 also provides great value in supporting an embarked coalition commander and his staff. Like the Talon, the SecNet54 can be keyed to a CENTRIXS enclave, allowing all hosts connected to the SecNet54 to access all classified data available to that particular CENTRIXS enclave. This information includes coalition releasable classified e-mail, documents, and chat. Additionally, a Voice-over IP (VoIP) phone can be attached to the commercial switch that is connected to the SecNet54, providing for coalition releasable classified voice communications.

The characteristic differences of the Talon and the SecNet54 depicted above indicate each SCTD is ideal for a different type of employment with a distinctly different group of users. These considerations must be taken into account prior to planning, acquiring, and deploying an SCTD solution.

## C. SECURITY REQUIREMENTS

Although SCTD technology provides an efficient means to extend the classified network to virtually any space on a wireless-LAN enabled ship, there are security requirements that must be met prior to employing an SCTD enabled host. Information assurance and systems security must be considered by both the technicians and the users of the classified hosts.

### 1. Physical Security

It is the responsibility of the user of an SCTD enabled host to maintain the security of that host. As discussed in Chapter II, both SCTDs are considered a Controlled Cryptographic Item (CCI)—that is, they are unclassified but accountable. As CCI, they must be physically maintained on a person or in a GSA approved safe or facility certified to secure classified information [26]. The security of the SCTD is not the only consideration, however. The host itself must be handled at the highest classification level of the data that it has accessed or will be maintained on that host. Since the host is a computer, with a processor, memory, and storage, the classified data remains on the host. It is this quality of the host that dictates that it be handled at the classification level of the data. The host must be accounted for at all times, never being left unattended by an authorized, cleared user. When not being used, the host must be stored in a certified safe or storage facility

When deploying either SCTD in a shipboard space, great care must be taken as to the classification access level of the personnel that have access to that space. The user is responsible to ensure that no person could view or access information made available by the SCTD enabled host that does not have the proper clearance and a need-to-know. By allowing non-cleared personnel in the space, there is a potential for classified data

compromise as a result of shoulder surfing, where an unauthorized individual uses direct observation techniques to find out information. This information could be in the form of text from e-mail, COP data, or collaboration tools. Worse yet, a username and password could be gleaned to logon to the system for future exploitation.

To mitigate the physical risks to the system, standard practices must be followed. Securing the SCTD and the host when not in use or maintaining positive control by an authorized user must be enforced through command policy and practice. Preventing unauthorized access to the data provided by the SCTD enabled host, whether incidental or malicious, can be achieved through securing the space in which the host is being used. By controlling the access to the space, the risk of compromise is reduced to acceptable levels.

### 2. Administrative Controls

As directed by the Secretary of the Navy in Instruction 5510.36A, every Department of the Navy command will establish an Information Security Program that meets, at a minimum, the policies set forth in the Information Security Manual [26], [27]. It is the policies that a command generates, as directed by the Secretary of the Navy, which provides the foundation for the protection of the command's information.

Examples of these controls include determination of who has the requisite clearances and further refining that list to include only those with a need to know [26]. By providing accounts and passwords to only those individuals that require access to the system, the attack surface is decreased, with fewer accounts being available to attempt to exploit.

### 3. Logical Controls

With each SCTD, the user must logon to the device in order to enable tunneling of data. Until a session is established, there is no data transmission between the network and the device. An assigned username and password is an example of the logical controls used in the extension of the network through the use of the SCTDs. This separate username and password scheme is also a matter of defending the network through a

Defense-in-Depth approach. On initial logon, the user establishes a connection with the tunneling device which permits a connection to the classified network, but does not allow access to network resources. At this point, the user must authenticate against the classified domain using his username and password associated with his resources on the network. In other words, just because users have access to the resources on the ship's SIPRNet does not mean that they may necessarily have an account that would gain them access to the tunneling capability. Conversely, if a user were to gain access to the tunneling device, but did not have access to the ship's SIPRNet, he would still not be able to access resources found on the ship's classified domain.

Additional logical controls would be enforced at the domain level, maintaining the same controls that are implemented throughout the classified wired network. This allows further segregation of network resources so fewer personnel would have access, again minimizing the potential attack surface. As an example, personnel from the Intelligence Department would be the only authorized users to gain access to a particular set of documents under an Intel file share.

With prudent implementation of these controls, potential risks introduced by the use of SCTD enabled hosts to extend the classified network are reduced to acceptable levels. That is to say, if a commander has a functioning and acceptable Information Security Program in place and his personnel are properly trained on the requirements of the program, there should be little concern in the commander's mind about extending his classified network to enhance command and control.

## D. UTILITY TO COMMAND AND CONTROL

The utility of using either SCTD is that it extends the classified network to where it is needed. Although it will benefit ship's company to have classified access in spaces that would not otherwise have such access, the purpose of this thesis is to demonstrate the value, if any, of SCTD utility to command and control, and thereby its potential for improving support for an embarked commander.

Command and control is an operational art made up of six elements. These elements include maintaining alignment, providing situational awareness, advancing the

plan, complying with procedures, countering the enemy, and adjusting apportionment. These elements are inherent in every warfare area—air defense, surface warfare, submarine warfare, information operations, and others [3]. To exercise command and control at a speed that will allow the commander to address these elements faster than the enemy commander can react, the correct support systems must be in place and able to meet the commander's requirements.

The employment of an SCTD solution allows the embarked commander and his staff to efficiently address each element of command and control from any space onboard the flagship. In order to maintain alignment, the commander must be able to generate and promulgate his intent to his subordinate commanders. This is traditionally done through message traffic, and more currently through e-mail and collaboration tools, all of which can be accomplished using an SCTD-enabled host.

The hosts also are capable of providing situational awareness. By using a host that has a Common Operational Picture application installed, the device can tunnel to the COP server to get the data needed to update its COP software. This provides the necessary situational awareness required by the commander at near real time. This capability allows the commander to determine if enemy composition is as expected, friendly forces are in accordance with plan, and whether forces are executing according to his transmitted intent [3].

To advance the plan, the commander must be able to monitor execution of the plan and match that against the timeline. Further, he must be able to ascertain when there is deviation from the plan due to an unforeseen condition [3]. This can be achieved through the use of chat and collaboration tools that reside on the SCTD enabled device. From any space in his flagship, the commander and his staff can receive the information about the change condition, adjust the plan accordingly, and transmit the new intentions all in order to move the plan forward.

Compliance with procedure is determined by the commander and his staff through the monitoring of plan execution. Compliance is ascertained by comparing the current execution with the plan as published in commander's intent, special instructions, and

operational orders. It is this compliance that provides for execution efficiencies and helps avoid friendly fire situations [3]. The capability to monitor compliance is achieved from the collaboration tools that are embedded in the SCTD hosts. From any space on the ship, the commander and his staff can monitor progress of the plan as reported in a chat client and view force disposition and progress from a generated COP.

To counter the enemy, timely and accurate intelligence information must be available to the commander and his staff at his C2 nodes to prepare the battle space. As the battle unfolds, and emerging intelligence, surveillance, and reconnaissance information becomes available, the commander can formulate counter operations. This depends on receiving reliable, accurate information at the C2 node [3]. By extending the shipboard classified network to assigned staff spaces, each staff cell has access to the same information at the same time, leading to more efficient planning and operational execution.

Through monitoring of the battle, changes to enemy force disposition and tactics, or friendly asset availability will be noted by the commander. This information must be timely in order to allow the commander to adjust apportionment of all of his forces, communications, and time. As Admiral Willard notes, "Very often, the operational commander, who knows what is occurring in all warfare areas and can judge the consequences of a change in timing in one element, is in the best position to make the call" [3]. To be in the best position to make the call, the commander and his staff must have timely, accurate, and reliable information. This is not possible without that information being readily available to the commander at his C2 nodes. The KOV-26 and the KIV-54 both enhance the commander's command and control capability by extending or increasing access to the C2 network to his C2 nodes and staff workspaces.

## E. SUMMARY

In this chapter, we discuss the operational considerations for employing the KOV-26 Talon and the KIV-54 SecNet54. The characteristics of mobility, multiple hosts capability, and power source determined the preferred mode of deployment for each device. The KOV-26 is more mobile; with power being provided by the host, but can

only enable tunneling on one host. These characteristics make the Talon ideally suited to support the commander or his STAO. Conversely, the SecNet54 required an external power source, thereby reducing mobility. However, one KIV-54 could support tunneling of multiple hosts, making it ideal for setting up an enclave in a space to support staff planning and operations.

We also examined the potential risks of employing these devices throughout a shipboard environment. With proper mitigation, the risks are far outweighed by the value that these devices provide by extending the classified network to spaces that the commander and his staff can now utilize for the exercise of command and control.

# V. CONCLUSIONS AND RECOMMENDATIONS

## A. CONCLUSIONS

The demonstrations and evaluations of the KOV-26 Talon and the KIV-54 SecNet54 performed by the officers and crew of the USS Cole (DDG 67) during Trident Warrior 2011 illustrated the value of tunneling secret data through an unclassified wireless LAN. SCTD user surveys were completed to help quantify the value these devices provided as measured in *usability, availability,* and *persistence*.

The results of the user surveys showed that users were overwhelmingly positive in their critique of both SCTDs, with a greater than 90% positive score for each measured area. This indicates that in the opinions of the sampled SIPRNet users, the Talon and the SecNet54 performed adequately to extend a ships' classified network. By extending the classified network, ship's company technicians can rapidly and painlessly provide a C2 node in any space throughout the ship to support the requirements of the embarked commander and his staff.

## B. RECOMMENDATIONS FOR FUTURE RESEARCH

This thesis studied two Secret Client Tunneling Devices that were able to be used over an existing afloat wireless LAN to enhance command and control in spaces that did not previously support command and control from the wired SIPRNet. By tunneling classified data through the unclassified wireless pathway, SIPRNet hosts were able to transmit and receive classified data at speeds equal to or greater than that provided by the ship's existing wired SIPRNet. Although this configuration worked extremely well, there are questions that could be answered with further research.

This study looked at the KOV-26 and the KIV-54 tunneling data to and from a SIPRNet host in the form of a laptop. Both devices had to be physically connected to the laptop by PCMCIA port (KOV-26) or an Ethernet RJ-45 connection (KIV-54). Although a laptop provides mobility, it does not provide the most convenient form factor to be truly

mobile throughout a ship. A potential area of study would be to look at similar tunneling devices that would enable smaller mobile devices such as smart-phones or tablet computers to connect wirelessly and tunnel classified data across the wireless LAN.

No matter which form of hosts is implemented, there is a question of security that must be maintained in order to keep the confidentiality of the data intact. During this study, laptops were utilized to access classified data. Because the laptop handles data by storing information in RAM and on disk, the laptop itself is classified at the same level as that of the highest classification of handled data. However, it would be much easier to maintain security if the host itself could stay unclassified when it is not connected or logged onto a tunneling device. This idea is similar to current thin client architectures with the host device (dumb terminal) being capable of reaching back to the servers, through the wireless LAN, where storage, manipulation and processing of the classified takes place.

Because this thesis looked at the use of a shipboard wireless LAN with greater than 95% coverage of the ship, it would be beneficial to examine the use of such a system from the context of Electronic Warfare. Future work could explore questions such as: How does our potential reliance on these systems leave us vulnerable to exploitation or jamming? What is our concept of operations in a restricted Emissions Control (EMCON) environment? These future efforts may help in our understanding of how to best leverage local wireless communications aboard ship.

# APPENDIX A. TW11 SCTD OPERATOR INSTRUCTIONS

## A. KOV 26 OPERATOR INSTRUCTIONS

From [28].

**Secret Client Tunneling Devices - KOV-26 Talon User Procedures**

**Note**All usernames and passwords are provided on separate sheet of paper.

1. Turn on Dell laptop.
2. Log onto the computer.
3. Insert KOV-26 into the PCMCIA slot on left side of the laptop computer. The KOV-26 Talon log on screen will pop up.


**Figure 1: KOV-26 Talon Log On Screen.**

4. Log onto KOV-26 using provided username and password.
5. Connect D-link wireless adapter into the USB port **on the KOV-26 Talon**.
6. Connect to the wireless network using the KOV-26 Talon. To do this, navigate to Tools > WiFi Configuration.

**Figure 3: KOV-26 Talon Navigate to WiFi Configuration**

7. Then highlight the correct wireless profile (listed on provided paper) and click "Connect". The light on the Dlink adapter will be green once connected.

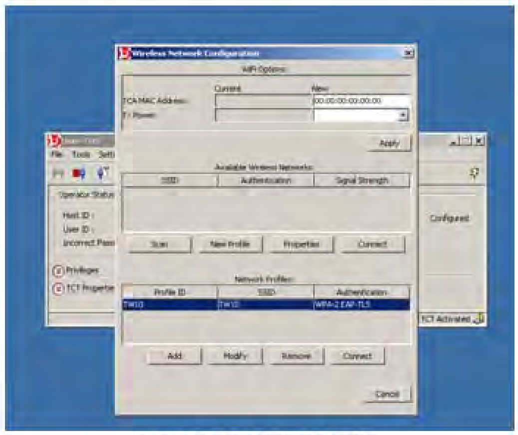


**Figure 4: Select Network Profile**

8. Close the Wireless Network Configuration window.
9. In Windows, navigate to Start > Run, type "cmd" and click ok.
10. On the command prompt, ping the SIPRNet to verify connectivity by typing "ping ________________" in the command prompt and hit enter. *It is normal for several pings to time out while the KOV-26 Talon is forming a security association with the SIPRNet gateway encryptor.
11. Once ping replies are received, close the command prompt.
12. Open Outlook.
13. Because it is your first time using this computer to access your SIPRNet email, it is necessary to set up Outlook. If you were to use this laptop again with this same user account, your email account would already be set up. To set up Outlook follow these steps:
    a. Click Next
    b. Click Yes
    c. Check the box for Manually Configuring your email account at the bottom, Click next
    d. Select Microsoft Exchange, Click Next
    e. Server address is: __________________; type in your last name and click "check name"
    f. One pop-up login screen, username is ddg67\"your SIPR login"; password is your SIPR password. Click OK
    g. Click Next
    h. Click Finish
    i. Several Microsoft popups will follow, do the following to click through them to your email Inbox

i. Popup One: Uncheck the box for online help and click OK
ii. Popup Two: Select the second option (no updates)
iii. Popup Three: Select No
iv. Popup Four: Select No

14. Log onto your email account.
15. Send "Talon Front" to yourself. This file is located in My Documents.
16. Click "Send/Receive" in Outlook Express.
17. Receive the email you sent to yourself. Open the attachment and verify completeness.
18. Send "Talon Quick Start Guide" to the second tester. The email address will be provided verbally. This document is located in My Documents.
19. Receive "Talon Quick Start Guide" from the second tester. The email address will be provided verbally. This document is located in My Documents.
20. Close Outlook.
21. Open Internet Explorer.
22. *Note: This website is saved in Favorites for Internet Explorer as Crypto Products and Services.* Navigate to http://infosec.navy.smil.mil/crypto/index.jsp?Topic=ine
23. At the top of the page is the KG-175D.
24. Click on the **KG-175D Micro Data Sheet** to open.
25. Verify download completeness by scrolling to end of document using the scroll bar on the right-hand side. This document has 2 pages
26. Close Internet Explorer.
27. Log off KOV-26 by navigating to File > Log Off on the User THS software.

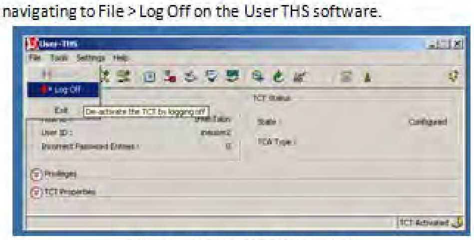



**Figure 6: Talon KOV-26 Log Off**

28. Shut down computer.
29. Unplug D-Link wireless adapter.
30. Remove KOV-26 Talon from laptop.

THIS PAGE INTENTIONALLY LEFT BLANK

## B. KIV 54 OPERATOR INSTRUCTIONS

### 1. Instructions for User 1

From [29].

**Secret Client Tunneling Devices – KIV-54 User 1 Procedures**

**Note**All usernames and passwords are provided on separate sheet of paper.

1. Turn on Dell laptop.
2. Log onto the computer.
3. If not already done, plug power adapter for KIV-54 into the wall and into rightmost port on KIV-54 when antennae are pointed away from you.
4. Turn on the KIV-54 by sliding the black power switch to ON.
5. Plug in Ethernet Cable from KIV-54 to switch.
6. Plug in one Ethernet cable from switch to laptop.
7. In Windows, navigate to Start > My Computer. Open the CD drive.
8. Open the folder called "Certificates". Double click the second certificate called "SecNet54_SSL_Client_Cert.p12"
9. On the Certificate Import Window, Click next twice. The password is secnet54 Click next twice more and then finish. On the two pop-up windows click Yes and then OK.
10. On the laptop, open Internet Explorer.
11. Type in https://____________________ into address bar and hit enter.
12. When certificate error appear, click Yes to continue
13. Login to KIV-54 webpage using provided login.
14. Click on XMOD on lefthand side of webpage.
15. Click "Enable RM01"
16. Once enabled, closed Internet Explorer.
17. In Windows, navigate to Start > Run, type "cmd" and click ok.
18. On the command prompt, ping the SIPRNet to verify connectivity by typing "ping _______________" in the command prompt. *It is normal for several pings to time out while the KIV-54 is forming a security association with the SIPRNet gateway encryptor.
19. Once ping replies are received, close the command prompt.
20. Open Outlook.
21. Because it is your first time using this computer to access your SIPRNet email, it is necessary to set up Outlook. If you were to use this laptop again with this same user account, your email account would already be set up. To set up Outlook follow these steps:
    a. Click Next
    b. Click Yes
    c. Check the box for Manually Configuring your email account at the bottom, Click next
    d. Select Microsoft Exchange, Click Next
    e. Server address is: _________________; type in your last name and click "check name"
    f. One pop-up login screen, username is ddg67\"your SIPR login"; password is your SIPR password. Click OK
    g. Click Next
    h. Click Finish
    i. Several Microsoft popups will follow, do the following to click through them to your email Inbox

i. Popup One: Uncheck the box for online help and click OK
ii. Popup Two: Select the second option (no updates)
iii. Popup Three: Select No
iv. Popup Four: Select No

22. Send "Talon Front" to yourself. This file is located in My Documents.
23. Click "Send/Receive" in Outlook Express.
24. Receive the email you sent to yourself. Open the attachment and verify completeness.
25. Send "Talon Quick Start Guide" to the second tester. The email address will be provided verbally. This document is located in My Documents.
26. Receive "Talon Quick Start Guide" from the second tester. The email address will be provided verbally. This document is located in My Documents.
27. Close Outlook.
28. Open Internet Explorer from the shortcut on the desktop.
29. Navigate to http://infosec.navy.smil.mil/crypto/index.jsp?Topic=ine This website is saved in Favorites for Internet Explorer.
30. At the top of the page is the KG-175D.
31. Click on the **KG-175D Micro Data Sheet** to open.
32. Verify download completeness by scrolling to end of document using the scroll bar on the right-hand side. This document has 2 pages
33. Close Internet Explorer.
34. Turn off KIV-54 and unplug it.
35. Shut down computer.

## 2. Instructions for User 2

From [30].

**Secret Client Tunneling Devices – KIV-54 User 2 Procedures**

**Note**All usernames and passwords are provided on separate sheet of paper.

1. Turn on Dell laptop.
2. Log onto the computer.
3. Plug in one Ethernet cable from switch to laptop.
4. In Windows, navigate to Start > Run, type "cmd" and click ok.
5. On the command prompt, ping the SIPRNet to verify connectivity by typing "ping _______________-t" in the command prompt. *It is normal for pings to time out while the KIV-54 is connecting to the wireless network and forming a security association with the SIPRNet gateway encryptor.
6. Once ping replies are received, close the command prompt.
7. Open Outlook.
8. Because it is your first time using this computer to access your SIPRNet email, it is necessary to set up Outlook. If you were to use this laptop again with this same user account, your email account would already be set up. To set up Outlook follow these steps:
    a. Click Next
    b. Click Yes
    c. Check the box for Manually Configuring your email account at the bottom, Click next
    d. Select Microsoft Exchange, Click Next
    e. Server address is: __________________; type in your last name and click "check name"
    f. One pop-up login screen, username is ddg67\"your SIPR login"; password is your SIPR password. Click OK
    g. Click Next
    h. Click Finish
    i. Several Microsoft popups will follow, do the following to click through them to your email Inbox
        i. Popup One: Uncheck the box for online help and click OK
        ii. Popup Two: Select the second option (no updates)
        iii. Popup Three: Select No
        iv. Popup Four: Select No
9. Send "Talon Front" to yourself. This file is located in My Documents.
10. Click "Send/Receive" in Outlook Express.
11. Receive the email you sent to yourself. Open the attachment and verify completeness.
12. Send "Talon Quick Start Guide" to the second tester. The email address will be provided verbally. This document is located in My Documents.
13. Receive "Talon Quick Start Guide" from the second tester. The email address will be provided verbally. This document is located in My Documents.
14. Close Outlook.
15. Open Internet Explorer from the shortcut on the desktop.
16. Navigate to http://infosec.navy.smil.mil/crypto/index.jsp?Topic=ine This website is saved in Favorites for Internet Explorer.
17. At the top of the page is the KG-175D.
18. Click on the **KG-175D Micro Data Sheet** to open.
19. Verify download completeness by scrolling to end of document using the scroll bar on the right-hand side. This document has 2 pages
20. Close Internet Explorer.
21. Shut down computer.

THIS PAGE INTENTIONALLY LEFT BLANK

# APPENDIX B. TW11 SCTD SURVEYS

## A. KOV 26 OPERATOR SURVEY

From [24].

### IT_SCTD_KOV-26_Operator Survey

**1) Background Information**

Initials: ____________________
Your initials serve as your TW11 ID. Please enter your initials the same way every time you fill out a survey or log.

E-Mail: ____________________
We may want to interview you about your responses. If that's OK please provide your email address.

Date of Event: ____________________

Local Time: ____________________

Billet, Rank & Rate: ____________________

Platform / Site: ____________________
For example: USS Wasp, USS Cole, UARNOC.

Specific Location: ____________________
For example: Radio Room, Server Room #2.

**Technology being evaluated: <u>KOV-26</u>**

**2) What is your affiliation / relationship with this technology?**

- ○ I used it for the first time in TW 11
- ○ I have previous experience using this technology (prior to TW11)
- ○ I am on (or hired by) the development team
- ○ Other (please specify) ____________________

**3) How much experience or training do you have with this technology?**

____________________

**4) What is your level of proficiency on this technology?**

- ○ Novice
- ○ Intermediate
- ○ Advanced
- ○ Expert
- ○ Other (please specify) ____________________

**Please consider your experience with KOV-26 during Trident Warrior 2011 as you respond to the following items:**

**5) How easy / difficult was it to use KOV-26 to enable the wireless connection?**

- ❍ Very Easy
- ❍ Easy
- ❍ Difficult
- ❍ Very Difficult
- ❍ N/A

**6) Please rate the amount of time required to connect to the wireless network with KOV-26 (rate the length of time from when you first powered on the Laptop).**

- ❍ Faster than expected
- ❍ Adequate
- ❍ Slower than expected
- ❍ N/A

**7) How many attempts were required to make the first connection to the wireless network?**

- ❍ 1
- ❍ 2
- ❍ 3
- ❍ 4
- ❍ 5 or more
- ❍ was not able to connect
- ❍ N/A

**8) Please describe any problems you had connecting to the wireless network.**

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

**9) Once connected to the wireless network, was the connection maintained during the entire session?**

- ❍ Yes
- ❍ No
- ❍ was not able to make initial connection
- ❍ N/A

**10) If the connection was lost during the session, how many times was it lost?**

- ❍ 1
- ❍ 2
- ❍ 3
- ❍ 4
- ❍ 5 or more
- ❍ was not able to reconnect
- ❍ N/A

**11) Please describe any problems you had maintaining a network connection. In particular, please report whether the session had to be terminated early due to connectivity problems.**

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

**12) Compared with your typical daily experience with Outlook, rate the time required to send and receive emails <u>with small attachments</u> (< 1MB) using the wireless connection with KOV-26.**

- ❍ Faster than normal
- ❍ About the same
- ❍ Slower than normal
- ❍ N/A

**13) Compared with your typical daily experience with Outlook, rate the time required to send and receive emails <u>with large attachments</u> (> 1MB) using the wireless connection with KOV-26.**

- ❍ Faster than normal
- ❍ About the same
- ❍ Slower than normal
- ❍ N/A

**14) Please describe any problems you had receiving or sending emails with Outlook Express over the wireless network.**

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

**15) Were you able to use Internet Explorer to open the specified website?**

- ❍ Yes
- ❍ No
- ❍ N/A

**16) If you were able to open the specified website, how did the webpage load – i.e., was it complete with good quality graphics?**

- ❍ No problems loading
- ❍ Minor problems loading
- ❍ Major problems loading
- ❍ N/A

**17) Compared with your typical daily experience with web browsers, rate the time required to load the webpage.**

- ❍ Faster than normal
- ❍ About the same
- ❍ Slower than normal
- ❍ N/A

**18) Were you able to use Internet Explorer to download the specified user manual?**

- ❍ Yes
- ❍ No
- ❍ N/A

**19) If you were able to download the specified use manual, how did the manual load – i.e., was it complete with good quality display of contents?**

- ❍ No problems loading
- ❍ Minor problems loading
- ❍ Major problems loading
- ❍ N/A

**20) Compared with your typical daily experience with web browsers, rate the time required to download the manual.**

- ❍ Faster than normal
- ❍ About the same
- ❍ Slower than normal
- ❍ N/A

21) **Please describe any problems you had opening webpages or downloading files with Internet Explorer over the wireless network.**

____________________________________________________

____________________________________________________

____________________________________________________

____________________________________________________

22) **Using KOV-26 would improve my ability to complete SIPRNET tasks.**

- ❍ Strongly Agree
- ❍ Somewhat Agree
- ❍ Somewhat Disagree
- ❍ Strongly Disagree
- ❍ N/A

23) **Describe any concerns you have regarding SIPRNET access via an unclassified wireless connection.**

____________________________________________________

____________________________________________________

____________________________________________________

____________________________________________________

24) **Overall, how satisfactory was your experience with KOV-26?**

- ❍ Very Satisfactory
- ❍ Somewhat Satisfactory
- ❍ Somewhat Unsatisfactory
- ❍ Very Unsatisfactory
- ❍ N/A

25) **In what situations could the KOV-26 be utilized for your group?**

____________________________________________________

____________________________________________________

____________________________________________________

____________________________________________________

**26) What did you like MOST about KOV-26?**

________________________________________________

________________________________________________

________________________________________________

________________________________________________

**27) What did you like LEAST about KOV-26?**

________________________________________________

________________________________________________

________________________________________________

________________________________________________

**28) What features or capabilities, if any, would you add, remove or change to improve KOV-26?**

________________________________________________

________________________________________________

________________________________________________

________________________________________________

*Thank you for your responses. Your input is very valuable to the success of TW-11.*

## B. KIV 54 OPERATOR SURVEY

From [31].

# IT_SCTD_KIV-54_Operator Survey

**1) Background Information**

Initials: ____________
Your initials serve as your TW11 ID. Please enter your initials the same way every time you fill out a survey or log.

E-Mail: ____________
We may want to interview you about your responses. If that's OK please provide your email address.

Date of Event: ____________

Local Time: ____________

Billet, Rank & Rate: ____________

Platform / Site: ____________
For example: USS Wasp, USS Cole, UARNOC.

Specific Location: ____________
For example: Radio Room, Server Room #2.

**Technology being evaluated: KIV-54**

**2) What is your affiliation / relationship with this technology?**

- O I used it for the first time in TW 11
- O I have previous experience using this technology (prior to TW11)
- O I am on (or hired by) the development team
- O Other (please specify) ____________

**3) How much experience or training do you have with this technology?**

____________

**4) What is your level of proficiency on this technology?**

- O Novice
- O Intermediate
- O Advanced
- O Expert
- O Other (please specify) ____________

**Please consider your experience with KIV-54 during Trident Warrior 2011 as you respond to the following items:**

**5) How easy / difficult was it to use KIV-54 to enable the wireless connection?**

- O Very Easy
- O Easy
- O Difficult
- O Very Difficult
- O N/A

**6) Please rate the amount of time required to connect to the wireless network with KIV-54 (rate the length of time from when you first powered on the Laptop).**

- O Faster than expected
- O Adequate
- O Slower than expected
- O N/A

**7) How many attempts were required to make the first connection to the wireless network?**

- O 1
- O 2
- O 3
- O 4
- O 5 or more
- O was not able to connect
- O N/A

**8) Please describe any problems you had connecting to the wireless network.**

____________________________________________________________

____________________________________________________________

____________________________________________________________

____________________________________________________________

**9) Once connected to the wireless network, was the connection maintained during the entire session?**

- O Yes
- O No
- O was not able to make initial connection
- O N/A

10) If the connection was lost during the session, how many times was it lost?

- ○ 1
- ○ 2
- ○ 3
- ○ 4
- ○ 5 or more
- ○ was not able to reconnect
- ○ N/A

11) Please describe any problems you had maintaining a network connection. In particular, please report whether the session had to be terminated early due to connectivity problems.

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

12) Compared with your typical daily experience with Outlook, rate the time required to send and receive emails with small attachments (< 1MB) using the wireless connection with KIV-54.

- ○ Faster than normal
- ○ About the same
- ○ Slower than normal
- ○ N/A

13) Compared with your typical daily experience with Outlook, rate the time required to send and receive emails with large attachments (> 1MB) using the wireless connection with KIV-54.

- ○ Faster than normal
- ○ About the same
- ○ Slower than normal
- ○ N/A

14) Please describe any problems you had receiving or sending emails with Outlook Express over the wireless network.

________________________________________________________________

________________________________________________________________

________________________________________________________________

________________________________________________________________

**15) Were you able to use Internet Explorer to open the specified website?**

- O Yes
- O No
- O N/A

**16) If you were able to open the specified website, how did the webpage load – i.e., was it complete with good quality graphics?**

- O No problems loading
- O Minor problems loading
- O Major problems loading
- O N/A

**17) Compared with your typical daily experience with web browsers, rate the time required to load the webpage.**

- O Faster than normal
- O About the same
- O Slower than normal
- O N/A

**18) Were you able to use Internet Explorer to download the specified user manual?**

- O Yes
- O No
- O N/A

**19) If you were able to download the specified use manual, how did the manual load – i.e., was it complete with good quality display of contents?**

- O No problems loading
- O Minor problems loading
- O Major problems loading
- O N/A

**20) Compared with your typical daily experience with web browsers, rate the time required to download the manual.**

- O Faster than normal
- O About the same
- O Slower than normal
- O N/A

21) Please describe any problems you had opening webpages or downloading files with Internet Explorer over the wireless network.

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

22) Using KIV-54 would improve my ability to complete SIPRNET tasks.

- O Strongly Agree
- O Somewhat Agree
- O Somewhat Disagree
- O Strongly Disagree
- O N/A

23) Describe any concerns you have regarding SIPRNET access via an unclassified wireless connection.

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

24) Overall, how satisfactory was your experience with KIV-54?

- O Very Satisfactory
- O Somewhat Satisfactory
- O Somewhat Unsatisfactory
- O Very Unsatisfactory
- O N/A

25) In what situations could the KIV-54 be utilized for your group?

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

**26) What did you like MOST about KIV-54?**

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

**27) What did you like LEAST about KIV-54?**

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

**28) What features or capabilities, if any, would you add, remove or change to improve KIV-54?**

______________________________________________________________

______________________________________________________________

______________________________________________________________

______________________________________________________________

*Thank you for your responses. Your input is very valuable to the success of TW-11.*

## C. KOV 26 SME OBSERVATION LOG

From [32].

**IT_KOV-26_SME_ObsLog**

Billet, rate & rank of the KOV-26 operator: ____________________

Observer Name: ____________________ Date & Local Time: ____________________ Location: ____________________

**Items preceded by '*' – ask the user how the latencies with SCTD compare to the latencies typically experienced.**

| STEP | Comments and Guided Responses |
|---|---|
| ***User turns on laptop and logs on.*** <br>• Able to power on & log on?.................. | |
| ***User plugs in KOV-26 and plugs in wireless adapter to KOV-26*** <br>• Any problems with the plug-in process? Please describe ................................ | |
| ***User logs into the KOV-26.*** <br>• Any problems with the log-in process? Please describe ................................ | |
| ***User selects the wireless network.*** <br>• Did the user find & select the network? | |
| • Did the RADIUS Server authenticate the wireless certificate?........................... | |
| • Was a connection established?............. | |
| • How many attempts were required to make the first connection?.................. | |
| • Any problems establishing a connection? Please describe ................ | |
| • *What was the user's assessment of the amount of latency? Approx time? ......... | |
| • For lost connection(s), how many times did the user have to reconnect? | |
| ***User pings the email server.*** <br>• Was a Security Association created? | |
| ***User opens Outlook and receives an email sent by another user*** <br>• Was the user able to open Outlook?...... | |
| • Was the user able to receive the email? | |
| • *What was the user's assessment of the amount of latency? Approx time? ......... | |
| What was the quality of display of the email?............................................. | |
| ***SIPR user sends an email to self with small attachment.*** | |
| • Was the user able to send and receive the email to self? ............................. | |
| • *What was the user's assessment of the amount of latency? Approx time? ........ | |

| STEP | Comments and Guided Responses |
|---|---|
| ***SIPR user sends an email to self with large attachment.*** <br>• Was the user able to send and receive the email to self? .............................. | |
| *What was the user's assessment of the amount of latency? Approx time? ......... | |
| ***User sends an email with a large attachment to another user account, and closes Outlook.*** <br>Was the user able to attach the file? ..... | |
| • Any problems attaching the file? Please describe ......................................... | |
| • Was the user able to send email to another user account? ........................ | |
| *What was the user's assessment of the amount of latency? Approx time? ......... | |
| ***SIPR user launches Internet Explorer and navigates to Infosec website.*** <br>• Was the user able to launch Internet Explorer? .......................................... | |
| • Was the user able to access the specified website?............................. | |
| • *What was the user's assessment of the amount of latency? Approx time? ......... | |
| • What was the quality of display of the website?.......................................... | |
| ***SIPR user downloads a specified user manual to the laptop desktop, and examines it for completeness.*** <br>• Was the user able to download the specified manual?............................. | |
| • *What was the user's assessment of the amount of latency? Approx time? ......... | |
| • Was the downloaded manual complete with good quality display of contents?... | |
| ***User closes Internet Explorer, then logs off and pulls out KOV-26. User turns off the laptop.*** <br>• Was user able to log off the KOV-26 Talon?............................................. | |
| • Was user able to remove KOV-26 Talon?............................................. | |
| • Any problems? Please describe ............ | |
| **Please report any connectivity problems that occurred during the session** | |

## D. KIV 54 SME OBSERVATION LOG

From [33].

**IT_KIV-54_SME_ObsLog**

Billet, rate & rank of the KIV-54 operator: ______________________________

Observer Name: ____________________ Date & Local Time: ____________________ Location: ____________________

**Items preceded by '*' – ask the user how the latencies with SCTD compare to the latencies typically experienced.**

| STEP | Comments and Guided Responses |
|---|---|
| ***User turns on laptop and logs on.*** • Able to power on & log on?................ | |
| ***User turns on KIV-54 and connects via the switch to the laptops.*** • Was user able to turn on KIV-54?....... | |
| • Any problems with the connection process? Please describe. ................. | |
| ***User logs into the KIV-54 webpage*** • Any problems with the log-in process? Please describe.............................. | |
| ***User enables KIV-54.*** • Did the user enable KIV-54? | |
| • Did the RADIUS Server authenticate the wireless certificate? ......................... | |
| • Was a connection established?........... | |
| • How many attempts were required to make the first connection?................ | |
| • Any problems establishing a connection? Please describe.............. | |
| • *What was the user's assessment of the amount of latency? Approx time?....... | |
| • For lost connection(s), how many times did the user have to reconnect?......... | |
| ***User pings the email server.*** • Was a Security Association created? | |
| ***User opens Outlook and receives an email sent by another user*** • Was the user able to open Outlook?.... | |
| • Was the user able to receive the email? | |
| • *What was the user's assessment of the amount of latency? Approx time?....... | |
| • What was the quality of display of the email? .......................................... | |
| ***SIPR user sends an email to self with small attachment.*** • Was the user able to send and receive the email to self?............................ | |
| • *What was the user's assessment of the amount of latency? Approx time?....... | |

| STEP | Comments and Guided Responses |
|---|---|
| ***SIPR user sends an email to self with large attachment.*** • .Was the user able to send and receive the email to self?............................ | |
| *What was the user's assessment of the amount of latency? Approx time?.......... | |
| ***User sends an email with a large attachment to another user account, and closes Outlook.*** Was the user able to attach the file?...... | |
| • .Any problems attaching the file? Please describe............................. | |
| • .Was the user able to send email to another user account?..................... | |
| *What was the user's assessment of the amount of latency? Approx time?.......... | |
| ***SIPR user launches Internet Explorer and navigates to Infosec website.*** | |
| • .Was the user able to launch Internet Explorer? ...................................... | |
| • .Was the user able to access the specified website? .......................... | |
| • .*What was the user's assessment of the amount of latency? Approx time?....... | |
| • .What was the quality of display of the website? ...................................... | |
| ***SIPR user downloads a specified user manual to the laptop desktop, and examines it for completeness.*** • .Was the user able to download the specified manual?........................... | |
| • .*What was the user's assessment of the amount of latency? Approx time?....... | |
| • .Was the downloaded manual complete with good quality display of contents? | |
| ***User closes Internet Explorer, then turns off KIV-54. User turns off the laptop.*** • .Was user able to carry out the close-down procedures? .......................... | |
| • .Any problems? Please describe .......... | |
| **Please report any connectivity problems that occurred during the session** | |

# LIST OF REFERENCES


[1] H. S. Kenyon. "At-sea wireless options continue to grow." *SIGNAL Online*, November 2009. Available: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2103&zoneid=277. [accessed February 15, 2011].

[2] B. Larson. "RE: USS COLE wireless LAN." Personal e-mail, August 22, 2011.

[3] R. F. Willard. "Rediscover the art of command & control." *Proceedings Magazine*, 128/10, p. 1196, October 2002. Available: http://www.usni.org/magazines/proceedings/2002–10/rediscover-art-command-control. [accessed March 11, 2011].

[4] M. Edwards, "Additional guidance WRT cancellation of moratorium on wireless networks," Naval administration message. Available: http://www.public.navy.mil/bupers-npc/reference/messages/Documents/NAVADMINS/NAV2006/NAV06283.txt. [accessed May 17, 2011].

[5] Department of the Navy Chief Information Officer, "DON CIO policy & guidance: DON use of commercial wireless local area network devices, services and technologies." Secretary of the Navy instruction. Available: http://www.doncio.navy.mil/Download.aspx?AttachID=782, [accessed August 12, 2011].

[6] 3e Technologies International, "Secure Wireless Infrastructure & Solutions." Product brief. Available: http://sis.saehan.co.kr/Upload/FILES/TWB/8/20090330_3.pdf. March, 2009 [accessed July 25, 2011].

[7] R. J. Suh. "Wireless content repurposing architecture for DC command and control." M.S. thesis, Naval Postgraduate School, Monterey, California, 2003.

[8] S. Hanceri. "Damage control and log taking Java applications for shipboard wireless LANs." M.S. thesis, Naval Postgraduate School, Monterey, California, 1999.

[9] A. Athanasopoulos, E. Topalis, C. Antonopoulos and S. Koubias. "Evaluation analysis of the performance of IEEE 802.11b and IEEE 802.11g standards," presented at *Networking, International Conference on Systems and International Conference on Mobile Communications and Learning Technologies*, 2006.

[10] D. Coleman and D. Westcott, *Certified Wireless Network Administrator.* Indianapolis, IN: Wiley Publishing, 2009.

[11] L-3 Communications Communication Systems-East. *Talon User Manual*. Published manual. Available: https://infosec.nmci.navy.mil/crypto/documents/KOV26_manual.pdf. [June 17, 2011].

[12] Assistant Secretary of Defense for Command, Control, Communications, and Intelligence. *DoD 5200.1-R: Information Security Program.* Washington D.C.: Office of the Assistant Secretary of Defense, 1997.

[13] L-3 Communications Communication Systems-East. *Talon Manual for Site Security Officers.* Published manual. Available: https://infosec.nmci.navy.mil/crypto/documents/KOV26_SSO_manual.pdf. [June 17, 20011].

[14] National Security Agency-Information Assurance Directorate, "Information assurance directorate certificate: SecNet-54," National Security Agency, February 2, 2009.

[15] Harris Corporation–RF Communications Division, *User Manual for the KIV-54RM01*. Published manual. Rochester, NY: Harris Corporation, 2008.

[16] Harris Corporation–RF Communications Division, *Administrator Manual for the KIV-54RM01.* Rochester, NY: Harris Corporation, 2008.

[17] Harris Corporation–RF Communications Division, *Administrator Manual for the KIV-54EM01.* Rochester, NY: Harris Corporation, 2008.

[18] National Institute for Standards and Technology Information Technology Laboratory, *Federal Information Processing Standards Publication* 140–2. Available: http://csrc.nist.gov/publications/fips/fips140–2/fips1402.pdf, [Jun 17, 2011].

[19] National Security Agency, "NSA suite B cryptography - NSA/CSS," November 8, 2010. Available: http://www.nsa.gov/ia/programs/suiteb_cryptography/. [accessed July 13, 2011].

[20] J. P. Venema and J. Lee Yee Shu, "Investigation into the impacts of migration to emergent NSA suite B encryption standards," M.S. thesis, Naval Postgraduate School, Monterey, California, 2009.

[21] U.S. Fleet Forces Command. *Trident Warrior 2011 (TW11) Orientation Guide*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Tool%20Kit/11_TW11%20hard%20copy%20instruments/IT/IT_SCTD_KOV-26_SME_ObsLog.doc [accessed July 14, 2011].

[22] Anonymous. *KOV-26/KIV-54 Wireless Architecture Proposal*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Focus%20Areas/IT/KOV-26%20OV-1.png [accessed July 14, 2011].

[23] Anonymous. *KOV-26 Workflow Diagram (OV-5)*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Focus%20Areas/C2/images/C2–03%20KOV%20OV-5.png [accessed July 20, 2011] .

[24] TW11 Data Analysis Working Group. *IT SCTD KOV-26 Operator Survey*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Tool%20Kit/11_TW11%20hard%20copy%20instruments/IT/IT_SCTD_KOV-26_Operator%20Survey.doc [accessed July 20, 2011].

[25] Anonymous. *Secret client tunneling device workflow diagram C2F KIV-54*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Focus%20Areas/IT/IT-13.02%20OV6c.jpg [accessed July 20, 2011].

[26] Secretary of the Navy. *SECNAV Instruction M-5510.36: Department of the Navy Information Security Program*. Available: http://doni.daps.dla.mil/SECNAV%20Manuals1/5510.36.pdf [accessed June 19, 2011].

[27] Secretary of the Navy. *SECNAVINST 5510.36A: Department of the Navy (DON) Information Security Program (ISP) Instruction*. Available: http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05–500%20Security%20Services/5510.36A.pdf [accessed June 19, 2011].

[28] S. Koontz. "Secret client tunneling devices - KOV-26 talon user procedures." Unpublished survey, SPAWAR, Point Loma, CA.

[29] S. Koontz. "Secret client tunneling devices - KIV-54 user 1 procedures." Unpublished survey, SPAWAR, Point Loma, CA.

[30] S. Koontz. "Secret client tunneling devices - KIV-54 user 2 procedures." Unpublished survey, SPAWAR, Point Loma, CA.

[31] TW11 Data Analysis Working Group. *IT SCTD KIV-54 Operator Survey*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Tool%20Kit/11_TW11%20hard%20copy%20instruments/IT/IT_SCTD_KIV-54_Operator%20Survey.doc [accessed July 20, 2011].

[32] TW11 Data Analysis Working Group. *IT KOV-26 SME ObsLog*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Tool%20Kit/11_TW11%20hard%20copy%20instruments/IT/IT_SCTD_KOV-26_SME_ObsLog.doc [accssed July 20, 2011].

[33] TW11 Data Analysis Working Group. *IT KIV-54 SME ObsLog*. Available: https://fire8.nps.navy.mil/content/dav/nps/workspaces/TW11_PLANNING/Tool%20Kit/11_TW11%20hard%20copy%20instruments/IT/IT_SCTD_KIV-54_SME_ObsLog.doc [accessed July 20, 2011].

# INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Dr. Dan Boger
   Naval Postgraduate School
   Monterey, California

4. Dr. Douglas J. MacKinnon
   Naval Postgraduate School
   Monterey, California

5. Mr. John H. Gibson
   Naval Postgraduate School
   Monterey, California